

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06282527 A**(43) Date of publication of application: **07.10.94**

(51) Int. Cl.

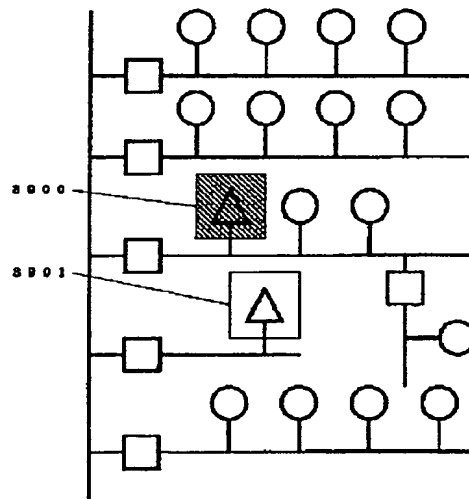
**G06F 15/00****G06F 15/00****G06F 13/00****G06F 15/16****H04L 12/24****H04L 12/26****H04M 3/42**(21) Application number: **05069751**(22) Date of filing: **29.03.93**(71) Applicant: **HITACHI SOFTWARE ENG CO LTD**(72) Inventor: **KONDOU MARIKO  
MORI YUMIKO  
TSUTSUMI TOSHIYUKI****(54) NETWORK CONTROL SYSTEM**

(57) Abstract:

**PURPOSE:** To detect a security hole on a network and to take measures for it.

**CONSTITUTION:** A security hole is detected in a network and the security hole is displayed on the constitution drawing of the network. Further, the display of the connection status from an external network, the access contents for an electronic computer and a network equipment, the access status to a setting file for maintaining network environments and the log-in status in a privileged user are displayed on the constitution drawing. The display is performed so that the difference may be recognized by the method how an electronic computer where all the monitoring programs are working is displayed by oblique lines like a code 3900 and an electronic computer having the monitoring programs which are not working is displayed by only a frame like a code 3901 or the method how colors are changed or display luminance is changed, etc., for instance.

COPYRIGHT: (C)1994,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平6-282527

(43) 公開日 平成6年(1994)10月7日

(51) Int. Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G06F 15/00	330	A 7459-5L		
	310	R 7459-5L		
13/00	351	Z 7368-5B		
15/16	470	M 9190-5L		
H04L 12/24				

審査請求 未請求 請求項の数10 O L (全30頁) 最終頁に続く

(21) 出願番号 特願平5-69751

(22) 出願日 平成5年(1993)3月29日

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会  
社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 近藤 麻里子

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会  
社内

(72) 発明者 森 優美子

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会  
社内

(74) 代理人 弁理士 秋田 収喜

最終頁に続く

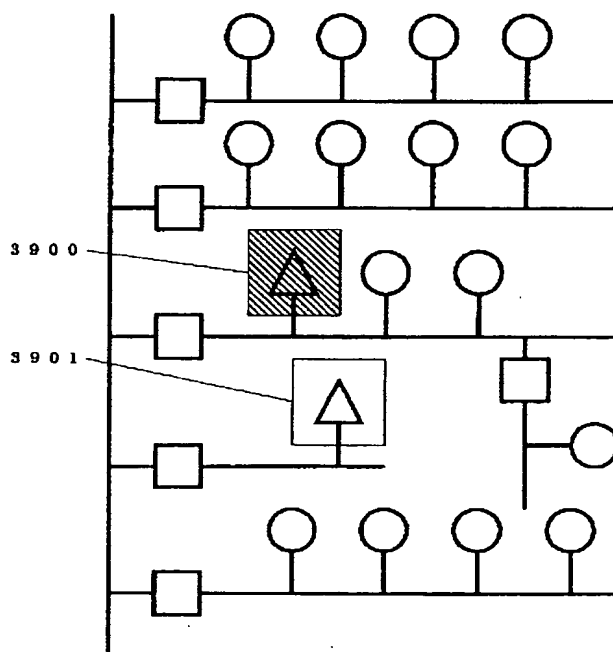
(54) 【発明の名称】 ネットワーク管理システム

(57) 【要約】 (修正有)

【目的】 ネットワーク上でのセキュリティホールを検出し、それに対する対策を講じる。

【構成】 ネットワークにおけるセキュリティホールを検出し、ネットワークの構成図面上に当該セキュリティホールを表示する。さらに、前記構成図面上に外部ネットワークからの接続状況表示、電子計算機及びネットワーク機器に対するアクセス内容、ネットワーク環境維持用設定ファイルへのアクセス状況、特権ユーザでのログイン状況を表示する。例えば、監視プログラムが全て稼働している電子計算機は符号3900のように斜線で表示し、稼働していない監視プログラムのある電子計算機は符号3901のように枠のみで表示するといった方法や、色を変えたり、表示輝度を変えるなどの方法により、違いが判るように表示する。

図39



## 【特許請求の範囲】

【請求項1】 電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、

前記ネットワーク機器の物理的配置と接続関係に関する情報を格納したデータベースと、ネットワーク構成図等を表示する表示装置と、前記データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を前記表示装置に表示すると共に、前記ネットワークのセキュリティホールを検出し、ネットワークのセキュリティホールの内容や重要度等に応じた表示形態により、前記ネットワーク構成図面上にネットワークのセキュリティホールを表示する手段と、ネットワークのセキュリティホールに対する対策を講じる処理手段とを有するネットワーク管理システム。

【請求項2】 請求項1に記載のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワーク構成図面上の位置への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図等の情報を用いて動的かつ論理的な接続状況を表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項3】 請求項1に記載のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワークケーブルへの指示操作に対し、電子計算機、ネットワーク機器及びネットワークケーブルでの通信量を測定し、さらに通信内容の分類と分類別の通信量割合を算出し、その測定結果及び分類結果に基づき通信量の時間的な推移及び変化、全体の通信量に対する分類別の通信量割合を、前記表示装置上に識別可能な形式で表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項4】 請求項1に記載のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成等の情報を用いて、動的かつ論理的なユーザのログイン状況を検出して表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項5】 請求項1に記載のネットワーク管理システムにおいて、ネットワーク上の電子計算機及びネットワーク機器で定義されたネットワーク環境を保持する環境設定ファイルに対するアクセス履歴を随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記環境設定ファイルに対するアクセス履歴から一定期間内のものを抽出し、その抽出結果を前記表示装置上に表示する手段とを設けることを特徴とするネットワーク管理システム。

【請求項6】 請求項1に記載のネットワーク管理システムにおいて、ネットワーク上の電子計算機及びネットワーク機器で定義された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で現在稼働中であるプログラム及びコマンド群の中から前記条件に合致しないプログラム及びコマンド、合致していても外部からの侵入可能性のあるプログラム及びコマンド、内部での不正使用の可能性あるプログラム及びコマンドを随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記データベースに格納したプログラム及びコマンドの動作状況を前記表示装置上に表示する手段とを設けることを特徴とするネットワーク管理システム。

【請求項7】 請求項1のネットワーク管理システムにおいて、論理的または物理的なネットワーク構成図面を前記表示装置に表示させ、ネットワーク上の電子計算機及びネットワーク機器で定義された特権ユーザによるネットワークへのログイン履歴を随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記データベースに格納した特権ユーザによるネットワークへのログイン履歴から一定期間内のものを抽出し、その抽出結果を前記表示装置上に表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項8】 請求項1のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、電子計算機及びネットワーク機器で定義されたネットワーク接続用環境設定ファイルの内容を、予め前記データベースに格納されたネットワークへのアクセス許諾条件等の情報に基づき照合及び検査する手段と、その結果を前記表示装置上に表示し、さらに緊急度・重要度に応じて通知を行う手段とを設けることを特徴とするネットワーク管理システム。

【請求項9】 請求項1のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、予め前記データベースに格納された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で稼働可能なプログラム及びコマンド群の中から前記条件に合致しないプログラム及びコマンド、合致していても外部からの侵入可能性のあるプログラム及びコマンド、内部での不正使用の可能性あるプログラム及びコマンドがあるかどうかを照合及び検査する手段と、その結果を前記表示装置上に表示する手段とを設けることを特徴とするネットワーク管理システム。

【請求項10】 請求項1のネットワーク管理システム

において、前記ネットワーク構成図面上で、ネットワーク監視を行っている電子計算機及びネットワーク機器をセキュリティレベルに応じて識別可能な形式で表示する手段を設けることを特徴とするネットワーク管理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、複数の電子計算機及びネットワーク機器が接続されているコンピュータネットワークに関し、特に、ネットワークを円滑に運用管理するためのネットワーク管理システムに関するものである。

【0002】

【従来の技術】ネットワークの基盤となる通信技術の発達により、ここ数年の間に高速で信頼性の高いネットワーク構築が可能になったため、年々その規模は大きく、広域化が進んでいる。

【0003】現在、ネットワーク管理作業の効率化を図るための「ネットワーク管理ツール」と呼ばれるシステムが各社から提案されている。こうしたツールの共通点は、SNMP (Simple Network Management Protocol) やCMIP (Common Management Information Protocols) 等の通信プロトコルを用いたネットワークの管理を行うという点である。

【0004】プロトコルレベルのネットワーク管理機能とは、ネットワークトラフィックのモニタリング機能、モニタリング結果をまとめる統計処理機能、トラフィック異常時のアラーム発生機能などである。

【0005】また、ネットワークのセキュリティ管理システムに関しては、

(1) 特開昭 6 2 - 2 1 1 7 6 5 号公報の「コンピュータシステムの利用者チェック装置」

(2) 特開平 0 1 - 7 6 2 6 1 号公報の「情報処理システムの不正侵入判断方式」

(3) 特開平 0 1 - 1 9 6 6 5 5 号公報の「不正ログイン防止方式」

(4) 特開平 0 1 - 2 2 4 8 5 8 号公報の「コンピュータの不正アクセス防止方法及びそれに用いるボード装置」

(5) 特開平 0 1 - 2 9 3 0 4 0 号公報の「回線接続許可装置」

(6) 特開平 0 2 - 1 9 2 3 3 9 号公報の「ハッカー侵入防止方式」

(7) 特開平 0 3 - 2 5 8 1 5 2 号公報の「通信サービス方式」

(8) 特開平 0 2 - 3 6 4 5 6 号公報の「ハッカー防止装置およびそのキーワード作成方法」

などがある。

【0006】前記 (1) のコンピュータシステムの利用者チェック装置は、端末を使用する利用者に ID コード

を入力させ、その ID コードを端末側とホスト側の両方で暗号処理装置により 2 次暗号を生成し、両者の 2 次暗号を比較し、一致した場合に暗号処理コードを更新することで、容易にコンピュータシステムへの侵入を行えないようにするものである。

【0007】前記 (2) の情報処理システムの不正侵入判断方式は、接続要求を行った端末に対し利用者 ID コードを要求し、さらに、その端末に対し信号を送出する。利用者 ID コードから求められる予め記憶された信号往復時間と接続要求のあった端末までの信号往復時間とを比較し、所定時間差以外の場合に接続を拒否するものである。

【0008】前記 (3) の不正ログイン防止方式は、不正なログイン試行を検出する手段及び不正ログインに対し疑似動作を行う手段を用い、侵入者の操作を監視し、ログイン時間を長引かせることで、ホストコンピュータへの侵入を防止するものである。

【0009】前記 (4) のコンピュータの不正アクセス防止方法及びそれに用いるボード装置は、コンピュータへのアクセス時に 2 つ以上のコード入力を促し、全てのコード入力終了した時点で正誤判定を行い、組合せの数を大きくさせ、不正アクセスを目的としたハッカーのコード検索を困難にさせるものである。

【0010】前記 (5) の回線接続許可装置は、接続可否情報を予め設定し、接続要求メッセージが入力された時点で、この情報に基づき接続可否判定を行うことで、コンピュータ装置への不正アクセスを防止するものである。

【0011】前記 (6) のハッカー侵入防止方式は、電話回線を用いた端末のコンピュータ接続時に、端末から暗証番号を 2 度入力させ、一定時間内に正しい暗証番号が送信されなければ、回線を切断するものである。

【0012】前記 (7) の通信サービス方式は、公衆回線網を用いたネットワークシステムにおいて、暗号 ID 発生機能付電話機から送付される装置 ID 及び暗号 ID を、予め登録してある加入者側の装置 ID 及び暗号 ID と比較することで、通信サービス許可の可否判定を行い、特定加入者のみに通信サービスを提供するものである。

【0013】前記 (8) のハッカー防止装置およびそのキーワード作成方法は、端末からホストに送信するデータに、端末 ID とパスワード、さらに、端末側で作成するキーワードを付加し、ハッカー防止装置によりキーワードの照合を行い、不一致の場合には回線を切断することで、バグ混入プログラム等の送信を防止するものである。

【0014】

【発明が解決しようとする課題】しかしながら、前記従来の技術では、以下に挙げるような問題がある。

【0015】(1) ネットワークのセキュリティホール

## の検出と対策

電子計算機及びネットワーク機器をネットワーク接続して使用する場合、どこかの端末からでも同様のサービスと使い易い環境を提供することと、外部からの侵入やネットワーク環境の不正使用防止は、相反する場合が多い。言い換えると、ネットワークの構築はセキュリティホールを作り出すことであるとも言える。

【0016】そこで、前記従来技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、不当なアドレスを有する接続機器の検出や、ネットワーク上を流れているデータのログ内容から不正なネットワーク利用者の検出を行う機能を有しているものがある。しかし、こうしたシステムでは、ネットワークのどの部分がセキュリティホールとなったかが把握できない。

【0017】すなわち、ネットワークに関する各種の設定条件等が実際に安全な設定になっているか、或は、使い易さのために部分的にセキュリティチェックを緩和させていないかといったことを、自動的に検出することができない。したがって、セキュリティ確保のための対策を予め講じておくことも困難になる。

【0018】さらに、前記従来技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、論理的な接続関係に基づくネットワーク構成図を表示するものが一般的であり、機器の物理的な配置（レイアウト）、例えば、どのビルの何階のどの部署のどの位置で接続しているかを表示できるものはない。

【0019】（2）外部からの侵入、内部での不正利用の早期発見

ネットワークに対する外部からの侵入及び内部での不正利用を完全に防止することは、現在の技術ではまだ困難である。しかし、その可能性をできるだけ低くするために、前記従来技術で述べたように、セキュリティ管理を行う各種の方式や装置が考えられている。

【0020】これらの方式や装置は、端末からのログイン時点、或は、回線接続時点での不正なアクセス防止を目的としている。しかし、これらの方式や装置では、ネットワークに侵入された後の不正利用を発見することはできない。

【0021】また、前記従来技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークトラフィックのモニタリング機能及びモニタリングのログ内容の統計処理機能を用いて、不当なアドレスを有する接続機器の検出や不正なネットワーク利用者の検出を行えるものもある。

【0022】しかし、こうしたシステムでは、実際に不正が行われ、管理者が何らかの異常な現象に気づき、ネットワークトラフィックのログ調査を開始するまでは、ネットワーク上のどこで何が行われているかを把握できず、早期発見が困難である。

【0023】さらに、こうした不正アクセス検出はトラ

フィックデータの内容に依存した方式で行われているため、ネットワーク利用者単位、利用者の実行権限単位、ネットワーク機器上で稼働しているコマンドやプログラムやプロセス単位、ネットワーク管理で使用するファイル単位、或は、ネットワーク機器単位で、不正アクセスを監視することができない。

【0024】（3）適正なネットワーク利用環境の構築支援

前記従来技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークの性能管理を行うために、ネットワーク上を流れるデータを収集し、その内容及び種別毎の統計処理を行う機能を有するものが多い。

【0025】しかし、性能管理を行うだけでは、適正なネットワーク利用環境を構築できない。すなわち、ネットワークに接続されている電子計算機、端末等を含むネットワーク機器をどのような条件や権限で使えるように設定しているかを把握することができない。

【0026】（4）安全なネットワーク環境の視覚的な把握

前記従来技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークの論理的な接続関係に基づくネットワーク構成図を表示し、接続しているネットワーク機器が稼働しているかどうかを表示する機能を有するものが多い。

【0027】しかし、そうしたネットワーク構成図の表示では、どのネットワーク機器でどのようなセキュリティ対策を講じているか、或は、どのネットワーク機器でどのような権限でどのようなコマンドやプログラムやプロセスが稼働しているかを視覚的に把握することができない。

【0028】本発明の第1の目的は、ネットワーク上でのセキュリティホールを検出し、ネットワーク構成図面上でそれを表示し、そのネットワークのセキュリティホールに対する対策を講じることができるネットワーク管理システムを提供することである。

【0029】本発明の第2の目的は、通常のネットワーク使用状況を常時監視し、一般のネットワーク利用者のネットワーク利用状況や、特権ユーザ権限でしか行えないシステム関連ファイルへのアクセスや、実行時に特権ユーザ権限を得ることのできる特定プロセスの稼働状況や、特権ユーザ権限でのネットワーク機器に対するアクセスを把握し、アクセスの記録を残すことで、外部からの侵入、内部での不正利用の早期発見を可能にすることができるネットワーク管理システムを提供することである。

【0030】本発明の第3の目的は、ネットワーク環境における様々なアクセス許諾内容の妥当性をチェックし、妥当でない場合はネットワーク管理者に通知を行い、適正なネットワーク利用環境の構築を支援すること

ができるネットワーク管理システムを提供することである。

【0031】本発明の第4の目的は、ネットワーク管理システムの管理対象となるネットワークをネットワーク構成図面上で表示することで、安全なネットワーク環境の視覚的な把握を行うことができるネットワーク管理システムを提供することである。

#### 【0032】

【課題を解決するための手段】前記第1の目的を達成するために、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納したデータベースと、ネットワーク構成図等を表示する表示装置と、前記データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を前記表示装置に表示すると共に、前記ネットワークのセキュリティホールを検出し、ネットワークのセキュリティホールの内容や重要度等に応じた表示形態により、前記ネットワーク構成図面上にネットワークのセキュリティホールを表示する管理手段と、ネットワークのセキュリティホールに対する対策を講じる処理手段とを設けた。

【0033】また、第2の目的を達成するために、本発明は、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワーク構成図面上の位置への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図等の情報を用いて動的かつ論理的な接続状況、即ち、現在、どの電子計算機又はネットワーク機器から、或はどんな外部のネットワークから、誰がどのような接続手段で、前記ネットワークに接続しているか、さらに動的なユーザのログイン状況表示、即ち、現在、どの電子計算機、端末、ネットワーク機器から、誰が、どの電子計算機及びネットワーク機器を使用し、どのような処理を行っているかの表示を行う手段とを設けた。

【0034】あるいは、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワークケーブル等を指示すると、電子計算機、ネットワーク機器及びネットワークケーブルでのネットワーク通信量を測定し、その測定結果に基づいた通信量の時間的な推移及び変化や、通信内容の分類を行い、分類別の通信量割合を算出し、測定結果及び分類結果に基づき、全体の通信量と全体の通信量に対する分類別の通信量割合を、前記表示装置上に識別可能な形式で表示する手段を設けた。

【0035】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義されたネットワーク環境を維持するための環境設定ファイルに対するアクセス履歴を随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記データベースに格納している

ネットワーク環境を維持するための環境設定ファイルに対するアクセス履歴から一定期間内のものを抽出し、その抽出結果、即ち、いつ、誰が、どのような変更・参照・追加を行ったかを前記表示装置上に表示する手段を設けた。

【0036】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で、現在、稼働中であるプログラム及びコマンド群の中から、前記条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものを随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記の条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものの動作状況を、前記表示装置上に表示する手段を設けた。

【0037】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義された特権ユーザによるネットワークへのログイン履歴を随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記データベースに格納している特権ユーザによるネットワークへのログイン履歴から、一定期間内のものを抽出し、その抽出結果、即ち、いつ、誰が、どこから、どの電子計算機及びネットワーク機器に対して、特権ユーザ権限で何を行ったかを前記表示装置上に表示する手段を設けた。

【0038】また、前記第3の目的を達成するために、前記前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、電子計算機及びネットワーク機器で定義されたネットワーク接続用環境設定ファイルの内容を、予め前記データベースに格納されたネットワークへのアクセス許諾条件等の情報に基づき、外部からの不正な侵入や不正な使用を許す環境になっていないかを、照合及び検査し、その結果を前記表示装置上に表示し、さらに、緊急度・重要度に応じ、ネットワーク管理者に対して通知する手段を設けた。

【0039】あるいは、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、予め前記データベースに格納された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で稼働可能なプログラム及びコマンド群の中から、前記条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものがあるかどうかを、照合及び検査し、その結果、即ち、どの機器

で、どのような危険な稼働可能なプログラム及びコマンド等があるかを前記表示装置上に表示する手段を設けた。

【0040】また、前記第4の目的を達成するために、物理的なネットワーク構成図面上で、ネットワーク監視を行っている電子計算機及びネットワーク機器を、セキュリティレベルに応じて識別可能な形式で表示する手段を設けた。

【0041】ここで、ネットワークのセキュリティホールとは、複数のネットワーク機器が接続しているネットワークにおける以下のような事項を指す。

(1) 外部ネットワークとの接続(アクセス) ポイント、(2) 外部ネットワークに対するアクセス許諾条件(論理的侵入可能性)、(3) ネットワーク上を流れる通信内容の偏り、(4) 特定ユーザ、プログラム、コマンド等によるネットワークの占有、(5) ネットワーク内に接続しているネットワーク機器を使用しているユーザが稼働させているプログラム及びコマンド群のセキュリティレベル及びユーザ権限、(6) ネットワーク内に接続している計算機以外のネットワーク機器のアクセス許諾条件、(7) ネットワーク内に接続しているネットワーク機器で定義された特権ユーザ権限での起動が可能なプログラム及びコマンドに対するアクセス許諾条件、(8) ネットワーク内に接続しているネットワーク機器の上記条件設定情報へのアクセス許諾条件、(9) ネットワーク内で稼働中のプログラム及びコマンド群のセキュリティレベル及びユーザ権限、(10) 特権ユーザ権限でのプログラム及びコマンドの起動、(11) 論理的に接続しているが、ネットワーク管理システムの管理対象範囲外の内部ネットワーク。

【0042】

【作用】前述の手段によれば、ネットワークのセキュリティホールを検出し、その検出したセキュリティホールをネットワーク構成図面上に表示するので、ネットワークにおけるセキュリティを確保することができる。

【0043】また、ネットワーク及びネットワーク機器に対するアクセス状況を常時監視するので、外部からの侵入、内部での不正利用の発見を速やかに行うことができる。

【0044】さらに、ネットワーク環境設定用ファイルの内容をアクセス許諾条件に基づき照合及び検査するので、適正なネットワーク利用環境の構築を容易に行うことができる。

【0045】さらに、ネットワーク管理の対象となっているネットワーク機器をネットワーク構成図面上で識別可能な形式で表示させるので、安全なネットワーク環境を視覚的に簡単に把握することができる。

【0046】

【実施例】以下、本発明の実施例を図面を参照して具体的に説明する。

【0047】図1は本発明の一実施例にかかるネットワーク管理システムの構成を示す図である。

【0048】図1において、100はネットワーク管理システムが管理する被管理機器がケーブル類で接続されたネットワークである。101は通信制御装置であり、ネットワーク管理システムとネットワーク100間の通信を制御する。

【0049】102は中央処理装置であり、データ処理、システム制御及び予めプログラムされた各種処理を行う。103は入力装置であり、キーボード、マウス、プリンタなどが用いられる。104は出力装置であり、ディスプレイ、プリンタなどが用いられる。105は、補助記憶装置であり、光磁気ディスク、メタルテープ、ハードディスクなどが用いられる。

【0050】なお、ネットワーク管理システムが管理する対象機器を、ここでは被管理機器と呼ぶ。この被管理機器は電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類、設備機器の6つに分類する。

【0051】電子計算機は、ワークステーションやパーソナルコンピュータやホストコンピュータやファイルサーバなどである。

【0052】端末は、X端末やキャタクタ端末やグラフィック端末などである。

【0053】ネットワーク機器は、ルータやリピータやターミナルサーバやトランシーバやブリッジやプロトコルコンバータやモデムなどである。

【0054】周辺機器は、プリンタやワードプロセッサやファクシミリやスキャナなどである。

【0055】ケーブル類は、イーサネットケーブルや電話線や電源ケーブルなどである。

【0056】設備機器は空調やフロアレイアウトや建屋地図などである。

【0057】また、ネットワークとは、被管理機器が接続されていて、各機器間で通信が行われているものである。

【0058】例えば、ワークステーション固有の属性としてCPU名、処理速度、クロック数、稼働OS、外部インターフェイス、MACアドレス、論理マシン名、IPアドレス、メモリサイズ、ハードディスク容量、増設ボードなどがあり、ルータ固有の属性には対応プロトコル、通信速度、ポート数、ポート形状、インターフェイス種類、拡張可能スロット数などがある。

【0059】ソフトウェア固有の属性には、製品名、バージョン、稼働OS、稼働環境、マニュアル、インストールマシン、保管場所、機能概要、バージョンアップ費用などが挙げられる。

【0060】ここに挙げた情報は、予め製品データベースに登録しておき、製品名と機種名を指定すれば必要な情報が得られるようになっている。

【0061】上述のような製品に関する情報以外に、ネ

ットワーク管理システムは、個々のコンピュータやネットワーク機器に固有の購入価格、購入先、購入年月、シリアル番号、修理履歴、保守費用なども管理属性として保持する。

【0062】さらに、ネットワーク管理システムは被管理機器である電子計算機や端末やネットワーク機器に関するソフトウェア環境、マシン環境、システム構成、ネットワークトラフィックなども管理属性として扱う。

【0063】また、本発明のネットワーク管理システムで扱う被管理機器の属性には、設備情報における地番、建屋名、フロア、面積、机位置、座席、マシン位置なども含まれる。

【0064】さらに、本発明のネットワーク管理システムでは以下に述べる手段を有する。

#### (1) ネットワーク設備データベース・インターフェイス

上述の対象となる被管理機器や各々の属性情報をデータベース化し、登録及び検索を行う。

【0065】この場合、各々の製品に固有の情報であるシリアル番号、保守契約の有無、購入先、保守契約などは、新規購入時にデータベース登録する。また、これらの属性情報データベースへのアクセス用ユーザインターフェイスがあり、どの端末からでも、どのデータに対しても同じようなインターフェイスで入力や更新が可能である。

#### 【0066】(2) 地図データベース

CADベースの図形処理を用いて、全国規模の地図情報からビル内のフロア単位の建屋図面まで階層化して保存する。上述のネットワーク設備データベースとリンクさせ、画面に表示した地図で機器の情報もアクセスできるユーザインターフェイスを提供する。

#### 【0067】(3) ハードウェア配置及びネットワーク配線管理

ネットワークの配線、接続状況、電源配置、マシンレイアウト、電話配線等を地図データベースに格納されている地図に基づいて作成する。

#### 【0068】(4) システム構成管理

新規にコンピュータを購入する場合に、必要な機器構成やソフトウェアの一覧を生成し、目的に合ったシステム構成になっているかチェックする。

#### 【0069】(5) マシン環境管理

例えば、ホームディレクトリはどこか、どのディスクに何が入っているか、マシンのシステム構成はどうなっているか、誰がアカウントを持っているか等の情報検索を可能にする。

#### 【0070】(6) ネットワーク環境管理

物理的な意味でのネットワーク環境の管理を行う。どこに、どんなマシンや端末が接続しているか、イーサネットでのネットワーク基準を満たしているかなどをチェックする。

#### 【0071】(7) ソフトウェア管理

ネットワーク上に接続された電子計算機及びネットワーク機器で稼働するソフトウェアの製品名、バージョン、稼働OS、稼働環境、マニュアル、インストールマシン、保管場所、機能概要、バージョンアップ費用などのソフトウェアに関する属性の管理を行う。

#### 【0072】(8) 物品在庫管理

未使用ケーブル、コネクタ、トランシーバ、ターミネータ等の数や貸し出しリストを管理する。

#### 【0073】(9) 統計処理

通信プロトコルレベルのネットワーク管理ツールと連動させ、定常的なネットワーク状況を監視し、ネットワークトラフィック、マシンのロードアベレージ、プリンタ稼働状況などの統計をとる。

#### 【0074】(10) ネットワーク敷設サポート

ネットワークの増設、機器追加、位置変更の際に、物理的なレベルで可否を診断する。例えば、電源供給量の過不足、コンセント数、イーサの制限長、接続可能な端末数などのチェックを行う。

#### 【0075】(11) ネットワーク監視

診断型エキスパートシステムと連動させ、障害発生時に障害箇所の特定を行ったり、回復のための対策指示を行う。また、ネットワークに接続されているマシンや端末を管理プロトコルの利用により自動検知する。さらに、ホストマシンやネットワークの負荷測定の結果から障害発生前に異常を検知し、ネットワーク管理者にアラーム通知する。

#### 【0076】(12) ネットワークインテグレイト

ここまで述べたネットワークに関する情報を総合的に判断し、円滑なネットワーク運営に何が不足しているか、どうすれば効率良いネットワークになるかのアドバイスをを行う。

【0077】ここで、本実施例で扱う用語、ネットワーク構成について説明しておく。

【0078】ネットワーク構成とは、電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類がどのように接続しているかを示すものである。実際の接続の位置関係や距離などを含む接続状況を示すものを物理的なネットワーク構成、サブネットやセグメントといった論理的な単位での接続状況を示すものを論理的ネットワーク構成と呼ぶ。

【0079】論理的なネットワーク構成図の例を図2に示す。図2の200は通信網、201は電子計算機、202はネットワーク機器、203は端末である。

【0080】一部の電子計算機には、ネットワークに接続されている別の電子計算機から送られてきた命令を実行し、その結果を送り返す機能がある。ネットワーク管理システムは、この機能を利用することで、ネットワークに接続されている電子計算機から情報を収集することができる。以下では、これを遠隔操作と呼ぶ。



【0081】次に、本実施例で用いるネットワーク構成図面について説明する。

【0082】ネットワーク構成図面とは、前記物理的ネットワーク構成と前記論理的ネットワーク構成を統括した図面であり、ある縮尺の地図、建屋図面、フロア図面上に、ネットワーク管理システムが管理する被管理機器を配置させ、同時にケーブル類の敷設状況や電源配置や電話配置なども含め、ネットワークの物理的な接続状況を実際の距離及び面積と合わせて表現したものである。

【0083】前記ネットワーク構成図面は、図示したい位置、範囲、被管理機器、セキュリティレベル、目的などに応じ、図1の補助記憶装置105内にあるデータベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図、ネットワークトラフィックの統計情報、ネットワーク回線使用率等の中から必要な情報を検索した上で、求められる情報を統合し、図1の出力装置104に表示される図面である。

【0084】本実施例で用いるネットワーク構成図面の例を図3に示す。

【0085】図3において、300は通信網、301はネットワーク機器、302は電子計算機、303は端末である。

【0086】ネットワーク管理システムは、上述の管理属性に関する情報を格納したデータベース以外に、以下に述べるデータベースをさらに有している。

【0087】図4は被管理機器の情報を格納したデータベース40の構造を示したものであり、400の被管理機器IDは被管理機器を一意に決めることのできる番号である。

【0088】この被管理機器ID400は、ネットワーク管理システムが表示するネットワーク構成図面の被管理機器図形データに割り当てられている。

【0089】401の接続情報は、物理的に直接接続している被管理機器の被管理機器IDである。

【0090】402の分類は、電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類を識別するものである。

【0091】403の遠隔操作は、遠隔操作の可能な被管理機器であるか判別する項目である。

【0092】404の管理者は、被管理機器を管理しているユーザのログイン名である。管理者は複数の場合もある。

【0093】図5はネットワーク環境を維持するために必要なファイル名の一覧が登録されているデータベース50の構造を示すもので、このデータベース50に格納している情報は、ネットワーク管理者であるネットワーク管理システムの利用者により予め登録されている。

【0094】ネットワーク上での被管理機器間の通信は、通信データを一定の長さに区切った情報単位により

行われている。これをパケットと呼ぶ。

【0095】図6にパケットの構成を示す。パケットは大きく2つの部分に分けることができる。すなわち、送受信するために必要な制御情報を格納しているヘッダ部60と実際に送受信したい情報を格納したデータ部61である。ヘッダ部60には、各種の制御情報が格納されているが、本発明の一実施例にかかるヘッダ情報は図示のように、受信先の被管理機器ID600、送信元の被管理機器ID601、パケットサイズ(バイト数)602、通信プロトコル603で構成されている。

【0096】ここから、被管理機器である電子計算機が、複数の別な電子計算機から遠隔ログインやファイル転送などでアクセスされている状態を表示する処理について、図7のフローチャートに沿って説明する。

【0097】ネットワーク上の遠隔処理が可能な全ての電子計算機は、常時ネットワークインタフェース上を送受信されるパケットのヘッダ部の一部を収集し記録している。これは、ネットワーク管理システムの遠隔操作として実行されている。

【0098】まず、ステップ700において、ネットワーク管理システムは、出力装置104にネットワーク構成を表示している。

【0099】ステップ701において、使用者により入力装置103から監視対象の電子計算機を指定する。

【0100】次にステップ702において監視期間を指定し、さらにステップ703において監視対象の電子計算機の被管理機器IDを用いて被管理機器情報を図4のデータベース40より検索する。

【0101】続く、ステップ704において、指定された電子計算機は遠隔操作が可能かどうかを調査する。遠隔操作が可能であれば、ステップ705へ、不可能であれば処理を終了する。

【0102】ステップ705においては、指定された電子計算機の被管理機器IDを用いて、ステップ702で指定された期間に収集したデータをネットワーク管理システムに送信する遠隔操作を実行する。

【0103】この時の収集データは、受信先被管理機器ID600、送信元被管理機器ID601、通信プロトコル603である。

【0104】図8に収集データの例を示す。800は受信先被管理機器ID、801は送信元被管理機器ID、802は通信プロトコルを示している。

【0105】次にステップ706において、出力装置104にステップ705で送信された収集データを結果として表示する。

【0106】次に、被管理機器を流れているパケットの通信プロトコル別の数量や数量比を表示する処理について図9のフローチャートに沿って説明する。

【0107】ネットワーク上の遠隔処理が可能な全ての電子計算機は、常時ネットワークインタフェース上を送

受信されるパケットのヘッダ部の一部を収集し記録している。これは、ネットワーク管理システムの遠隔操作として実行されている。

【0108】ステップ900において、ネットワーク管理システムは、出力装置104にネットワーク構成を表示している。次にステップ901において、使用者により入力装置103から監視対象の被管理機器を指定され、続くステップ902において使用者により監視期間が指定される。

【0109】ステップ903において、ステップ901で指定された被管理機器の被管理機器IDを用いて被管理機器情報を図4に示したデータベース40より検索する。

【0110】ステップ904において、検索した被管理機器が遠隔操作可能かどうかを調査する。

【0111】遠隔操作が不可能であればステップ905へ、可能ならばステップ906へ処理を進める。

【0112】ステップ905において、ステップ904で調べた被管理機器の接続情報を用いて、被管理機器の被管理機器情報を図4に示したデータベース40より検索する。

【0113】接続情報として複数の被管理機器IDがある場合は、先頭の被管理機器IDが使用される。

【0114】遠隔操作可能な被管理機器が見つかるまでステップ904、905の処理を繰り返す。

【0115】ステップ906において、ステップ904で検索した被管理機器の被管理機器IDを用いて、ステップ902で指定された期間に収集したデータをネットワーク管理システムに送信する遠隔操作を実行する。

【0116】この時の収集データは、パケットサイズ、通信プロトコルである。図10に収集データの例を示す。1000はパケットサイズ、1001は通信プロトコルである。

【0117】ステップ907において、図10の収集データより、通信プロトコル別にパケットサイズの合計を算出する。

【0118】ステップ908において、ステップ907で算出した通信プロトコル別パケットサイズの合計より、通信プロトコルのパケットサイズの総計を算出する。

【0119】ステップ909において、ステップ907の通信プロトコル別合計をステップ908の総計で割り、その数量比を算出する。

【0120】ステップ910において、出力装置にステップ907の結果とステップ909の結果をグラフで表示する。図11は棒グラフを用いた通信プロトコル別のパケット数量の合計の表示例、図12は円グラフを用いた通信プロトコル別のパケットの数量比の表示例を示すものである。なお、この他の表示形式をとってもよい。

【0121】次に、特定の端末や電子計算機の表示装置

(ここでは、まとめて端末と呼ぶ)で、どのユーザ名で、どの電子計算機にログインしているか、という情報を調査し表示する処理を、図2、図3、図14、図15を参照しながら図13のフローチャートにそって説明する。

【0122】図14はログイン記録テーブル140である。これは、各電子計算機へのログインを記録するテーブルであり、各電子計算機が保持している。このログイン記録テーブル140は、ログインしたユーザ名1400、そのログインで使用した仮想端末名1401、ログインした端末名1402、ログインした時刻1403、ログアウトした時刻1404、ログインする前のユーザ名(あるユーザにログインしてからログアウトせずにそこからユーザ名1400でログインした場合)1405が格納されている。ログイン中である場合、ログアウトした時刻1404は空欄である。

【0123】図15は、指定した端末で、どのユーザ名で、どの電子計算機にログインしているかを示す検出結果の表示例であり、電子計算機名1500、ログインしたユーザ名1501、そのログインで使用した仮想端末名1502、ログインした時刻1502が表示される。

【0124】まず、ステップ1300において、図2に示すような論理的なネットワーク構成図あるいは図3に示すような物理的なネットワーク構成図を表示する。

【0125】次にステップ1301において、システムの利用ユーザにより調査したい端末203が指定される。

【0126】次にステップ1302において、システムはネットワーク内の各電子計算機のログイン記録テーブル140を調査し、ステップ1301で指定された端末203からのログイン項目を検出する。

【0127】ステップ1302で検出するのはログイン中のもの(図14の1404が空欄のもの)である。また、仮想端末とは電子計算機側から見た論理的な端末(実際には1つの端末であるが、ソフトウェアでは複数の端末として扱うことをいう。例えば、複数のウィンドウのそれぞれを1つの端末として使用する場合に相当する。)意味し、一つのログインに対し一つの名前で割り当てられる。例えば、ある端末から複数ログインした場合、電子計算機側は複数の端末からログインされたと仮想して端末名を割り当てる。その個々の仮想的な端末を仮想端末と呼ぶ。

【0128】次に、ステップ1303において、システムは1302で検出した項目について、図15に示すように、電子計算機名1500、ユーザ名1501、仮想端末名1502、ログインした時刻1503をリストにして表示する。

【0129】次に、ネットワーク環境を維持していくために必要なファイルのアクセス履歴を監視する処理について図16、17のフローチャートに沿って説明する。

【0130】ネットワーク管理システムが、予め、アクセス履歴を保存するために実行している処理について図16のフローチャートに沿って説明する。

【0131】ステップ1600において、ネットワーク管理システムは、使用者によりアクセス履歴の保存期間を指定される。次に、ステップ1601において、図4に示したデータベース40より、遠隔操作可能な電子計算機の被管理機器情報を全て検索する。

【0132】ステップ1602において、検索した全ての遠隔操作可能な電子計算機の被管理機器IDを用いて、図5に示したデータベース50に登録されているファイルへのアクセス履歴情報を、ステップ1601で指定された期間、遠隔操作を行う電子計算機に保存する遠隔操作を実行する。

【0133】図18にアクセス履歴情報180の例を示す。ここで、1801はアクセスユーザ、1802はアクセス方法、1803はアクセス日時である。

【0134】次に、アクセス履歴を表示する処理について図17のフローチャートに沿って説明する。

【0135】ステップ1700において、ネットワーク管理システムは出力装置にネットワーク構成を表示している。ステップ1701において、使用者により入力装置で監視する電子計算機が指定される。ステップ1702において、指定された電子計算機の被管理機器IDを用いて被管理機器情報を図4に示したデータベース40より検索する。

【0136】ステップ1703において、指定された電子計算機が遠隔操作可能かどうかを調査する。遠隔操作ができればステップ1704へ、できなければ処理を終了する。

【0137】ステップ1704において、遠隔操作可能な電子計算機の被管理機器IDを用いて、図5に示したデータベース50のファイルのアクセス履歴情報をネットワーク管理システムに送信する遠隔操作を実行する。

【0138】ステップ1705において、ステップ1704においてネットワーク管理システムに送信されたアクセス履歴情報を出力装置に表示する。表示例を図19に示す。

【0139】次に、特権モードで稼働しているプログラムを捜し出して表示する処理を、図2、図3、図21、図23を参照して図20のフローチャートにそって説明する。

【0140】図21はプログラム起動ログテーブル210である。このプログラム起動ログテーブル210は、各電子計算機で起動されたプログラムの情報を記録するテーブルであり、各電子計算機が保持している。プログラム起動ログテーブルには図示のように、起動したユーザ名2100、起動されたプログラム名称2101、起動した仮想端末名2102、起動した端末名2103、起動時刻2104、終了時刻2105、起動時のモード

2106が格納されている。稼働中である場合、終了時刻2105は空欄である。

【0141】図22は特権モードで稼働中のプログラムを検出した結果の表示例であり、プログラム名2200、ユーザ名2201、起動した仮想端末名2202、起動した端末名2203、起動時刻2204が表示される。

【0142】特権モードのプログラムとは、他のプログラムやファイルに対して特権的な動作のできるプログラムである。特権的な動作の例としては、一般のユーザに対して書き込みを禁止しているファイルの書き換え動作や、他のユーザが起動しているプログラムの停止動作がある。

【0143】まずステップ2000において、図2に示したような論理的なネットワーク構成図、あるいは図3に示したような物理的なネットワーク構成図を表示する。

【0144】次に、ステップ2001において、システムのユーザにより調査したい電子計算機が指定される。

【0145】次に、ステップ2002において、ステップ2001で指定された電子計算機が有する図21に示すような全プログラム起動ログテーブルを調査し、特権モードで稼働しているプログラムを検出する。

【0146】ステップ2002で検出するのは、終了時刻が空欄であるもの、即ち、稼働中のものである。

【0147】次に、ステップ2003において、システムはステップ2002で検出したプログラムについて、プログラム名称2200、プログラムを起動したユーザ名2201、プログラムを起動した仮想端末名2202、プログラムを起動した端末名2203、プログラムの起動時刻2204をリストにして図22に示すように表示する。

【0148】次に、指定されたある期間中に、誰がどこで特権ユーザとなり、どのようなプログラムを動かしたかを調査し、表示する処理を図2、図3、図14、図21、図24、図25を参照して図23のフローチャートにそって説明する。

【0149】図24には、指定した期間内に、どのユーザ名からどの期間、特権ユーザにログインしていたかを表すテーブル240である。このテーブル240は、図23のフローチャートの処理途中で作成される。図24において、2400は仮想端末名、2401は端末名、2402はログインしていた時間帯、2403は特権ユーザにログインしたユーザ名である。指定された調査開始時刻以前に特権ユーザとしてログインしている場合は、調査開始時刻をログインした時刻として扱う。また、調査終了時刻以後に特権ユーザからログアウトしている場合は、調査終了時刻をログアウトした時刻として扱う。

【0150】図25は、ある期間に誰がどの端末で特権

10

20

30

40

50

ユーザとなり、どのようなプログラムを作動させたかを検出した結果の表示例であり、仮想端末名2500、ログインした端末名2501、起動時刻2503、終了時刻2504、ログインしたユーザ名2505が表示される。

【0151】電子計算機にログインする場合、通常の電子計算機利用を目的としたログイン名（以降では、これを一般ユーザと呼ぶ）か、電子計算機の管理を目的としたログイン名（以降では、これを特権ユーザと呼ぶ）のどちらかを使用する。

【0152】特権ユーザでログインすると、電子計算機上の全てのプログラムの起動や強制終了、全てのテーブル類の書き換えや消去などの特権的な動作が行える。

【0153】まずステップ2300において、図2に示したような論理的なネットワーク構成図、あるいは図3に示したような物理的なネットワーク構成図を表示する。

【0154】次にステップ2301において、システムのユーザにより調査したい電子計算機名と調査期間が指定される。

【0155】次に、ステップ2302において、システムはステップ2301で指定された電子計算機のログイン記録テーブル140（図14）を調査し、仮想端末名1401、端末名1402、ステップ2301で指定した期間において特権ユーザがログインした時間帯1403と1404、特権ユーザでログインする前のユーザ名1405を検出し、図24に示すような検出結果リストを作成する。

【0156】次に、ステップ2303において、ステップ2302で作成した検出結果リスト（図24）が空であるかを判断する。

【0157】ステップ2303が偽である場合は、ステップ2304において、検出結果リストの先頭項目の情報の特権ユーザがログインしていた時間帯と仮想端末名を用いて、時間帯2402に仮想端末2400で起動されたプログラムを、プログラム起動ログテーブル210（図21）から検出する。

【0158】ステップ2305において、ステップ2304で使用した先頭項目をステップ2302で作成した検出結果リストから削除し、ステップ2303に戻る。

【0159】ステップ2303が真である場合は、ステップ2305において、システムはステップ2304で検出した結果をまとめて図25に示すように仮想端末名2500、ログインした端末名2501、起動したプログラム名称2502、プログラム起動時刻2503、プログラム終了時刻2504、ログインしたユーザ名2505をリストにして表示する。

【0160】次に、ネットワーク環境を維持していくために必要なファイルのアクセス権の設定を検査する処理について、図27～図30を参照し、図26のフローチ

ャートに沿って説明する。

【0161】ネットワーク管理システムは、ファイルのアクセス権を、ファイル所有者、グループ所有者、その他の所有者のレベルに分けて行う。ファイル所有者は、ユーザ、グループ所有者はグループ、その他の所有者はファイル所有者、グループ所有者以外のユーザを示す。

【0162】ここでグループとは、複数のユーザをなんらかの目的でひとまとめにしたもので、例えば、あるプログラムの開発プロジェクトの全構成員とか、職制上の部長全員といったものになる。

【0163】ネットワーク管理システムは、ネットワーク環境を維持するため必要なファイルの本来あるべきアクセス権が登録されているデータベースを持っている。そのデータベース270を図27に示す。図27において、2700はファイル名、2701はファイル所有者に対するアクセス権、2702はグループ所有者に対するアクセス権、2703は上記以外のユーザに対するアクセス権、2704はファイル所有者、2705はグループ所有者を示している。

【0164】ここで例示しているファイルは、以下の設定を行う環境維持ファイルである。

【0165】まず、ファイル名2700の「/etc/passwd」はネットワークを使用する全ユーザが登録しているファイル名である。また、「etc/group」はユーザが属することができる全グループを登録しているファイル名である。さらに、「etc/hosts」はネットワーク上の電子計算機、ネットワーク機器、周辺機器を登録しているファイル名である。

【0166】図28はアクセス権の設定を説明する概念図であり、2800は読み、2801は書き、2802は実行のアクセス権を示すフィールドであり、ビットが1の時、許可されている。この図示の例では、読み、書きは許されているが、実行は許されていない。

【0167】図26のステップ2600において、ネットワーク管理システムは使用者により、ファイルのアクセス権の設定を検査する時間間隔、例えば1時間おき、3日間おき等の期間が指定される。

【0168】ステップ2601において、図4に示したデータベース40から、遠隔操作可能で、かつ電子計算機の管理者がネットワーク管理システムの使用者と同一のものを検索する。

【0169】ステップ2602において、ステップ2601で検索した全ての電子計算機に対して、被管理機器IDを用いて図5に示したデータベース50に格納されているネットワーク環境維持ファイルのアクセス権の設定状況を、ネットワーク管理システムに送信する遠隔操作を実行する。

【0170】図29はある電子計算機から送信されたアクセス権の設定状況の例である。

【0171】ステップ2603において、ステップ26

02で送信されたアクセス権の設定状況と図27に示したデータベースのアクセス権とを比較し、図30に示すような比較結果テーブル300を作成する。

【0172】図30において、3000は被管理機器ID、3001は比較を行ったネットワーク環境維持ファイル名、3002は送信されたアクセス権の設定状況、3003は本来あるべきアクセス権である。

【0173】比較の結果、相違がない場合は、被管理機器ID3000とファイル名3001のみが格納される。

【0174】次にステップ2604において、被管理機器の管理者に対して、ステップ2603で作成した比較結果テーブル300をメールで通知する。

【0175】ステップ2605において、ステップ2600で指定された期間、検査期間の設定変更がないか待つ。そして、ステップ2606において、ステップ2600で指定された期間情報が削除されるまでステップ2601からステップ2605の処理を繰り返す。

【0176】次に、一般ユーザが特権モードで起動できるプログラムを探し出して表示する処理を、図2、図3、図32～図34を参照し、図31のフローチャートにそって説明する。

【0177】図32は計算機中の全てのプログラムについてのプログラム状態テーブル320である。電子計算機には、一般モードで稼働するプログラムと特権モードで稼働するプログラムがある。またプログラムによって、所有者のみ起動可能、所有者と同じグループのユーザのみ起動可能など、起動者の制限もある。これらの稼働モードや起動者の制限に関する情報はプログラム状態テーブル320に格納されている。

【0178】プログラム状態テーブル320は図32に示すように、プログラム毎のプログラム名称3200、プログラムの所有者3201、起動可能なユーザ3202、稼働時のモード3203から成る。

【0179】このプログラム状態テーブル320は各電子計算機が保持している。

【0180】図33は、特権モードで起動できても支障のないプログラムのテーブル330で、これはネットワーク管理者によって登録される。特権モードで起動できても支障のないプログラムが事前に明らかな場合は、ネットワーク管理者は予め特権モードで起動できても支障のないプログラムをテーブル320に構成してシステムに登録して置く。ここではこれを事前登録テーブルと呼ぶ。

【0181】図34は一般ユーザが特権モードで起動できるプログラムについての検出結果の表示例である。

【0182】まず、ステップ3100において、図2に示したような論理的なネットワーク構成図、あるいは図3に示したような物理的なネットワーク構成図を表示する。

【0183】次に、ステップ3101において、ネットワーク管理者により一般ユーザが特権モードで起動できるプログラムの存在を調査したい電子計算機が指定される。

【0184】次に、ステップ3102において、システムはその電子計算機内のプログラム状態テーブル320を調査し、稼働時のモード3203が特権モードであるプログラムを検出する。

【0185】次に、ステップ3103において、事前登録テーブル330に登録されているかを判断する。ステップ3303が真であれば、ステップ3304において、事前登録テーブル330に登録されているプログラムの項目を、ステップ3102の検出結果から削除する。

【0186】次に、ステップ3105において、ステップ3102で検出したプログラム、又はステップ3104において項目削除を行った後のプログラムについて、図34に示すように、プログラム名称3400、プログラムの所有者3401、誰によって起動できるか3402をリストにして表示する。

【0187】また、ステップ3105において、リスト表示をシステムの出力装置に行うのではなく、ネットワーク管理者にメールで通知するののも一つの表示方法とする。

【0188】次に、監視プログラムがネットワーク上のどの電子計算機で稼働しているかを調査して表示する処理を、図2、図3、図36～図39を参照し、図35のフローチャートにそって説明する。

【0189】図36は、どのような監視プログラムを起動させているかを示すテーブル360で、ネットワーク管理者が登録したものである。

【0190】監視プログラムとは、外部からの侵入や不審なプログラムの稼働を監視したり、その結果を管理者に通知したりするプログラムのことであり、ネットワーク管理者が各電子計算機で稼働するように設定している。ネットワーク管理者は予め、図36に示すように、監視プログラムの稼働すべき電子計算機名3600と、その電子計算機で稼働すべき監視プログラム名3601と、その監視プログラムの重要度3602を格納したテーブル360を作成してシステムに登録しておく。このテーブルを監視プログラム登録テーブル360と呼ぶ。

【0191】図37、図38は調査対象指定の例、図39は監視プログラムが全て稼働中かの調査結果の表示例である。

【0192】まずステップ3500において、図2に示したような論理的なネットワーク構成図、あるいは図3に示したような物理的なネットワーク構成図を表示する。

【0193】次に、ステップ3501において、システムのユーザにより監視プログラムが稼働しているかどうか

かを調査するように指示される。調査対象の指示は、図37に示すような電子計算機3700の特定や、図38に示すような範囲指定3800などにより行う。

【0194】次に、ステップ3502において、指定された各電子計算機上でプログラム起動ログテーブル210（図21）を調査し、監視プログラム登録テーブル360（図36）に含まれるプログラムの稼働状況を検出する。

【0195】ステップ3503において、ステップ3500で表示したネットワーク構成図上で、指定された監視プログラムが全て稼働している電子計算機と、稼働していない監視プログラムのある電子計算機の違いが判るように表示する。例えば、図39に示すように、監視プログラムが全て稼働している電子計算機は符号3900のように斜線で表示し、稼働していない監視プログラムのある電子計算機は符号3901のように枠のみで表示するといった方法や、色を変えたり、表示輝度を変えるなどの方法により、違いが判るように表示する。

【0196】次に、ステップ3504において、図36のテーブル360で重要度3602が「大」と指定されている監視プログラムが全て稼働中であるかどうかを、ステップ3502の検出結果と監視プログラム登録テーブル360（図36）との比較により調査し、ステップ3504が偽である場合は、ステップ3505において、「重要度大」と指定されている監視プログラムが稼働していない旨を、メールや電話などで管理者へ直接通知する。

【0197】次に、ネットワーク管理システムがネットワーク上のセキュリティホールを検出後、検出したセキュリティホールへの対策を行う処理を、図40～図44を用いて、図45のフローチャートに沿って説明する。

【0198】図40はセキュリティホールテーブル400の内容を示す図である。セキュリティホールには、その内容に応じてセキュリティIDとセキュリティ対策IDが付けられている。図40の4000はセキュリティID、4001はセキュリティホール内容、4002はセキュリティ対策IDである。

【0199】図41はセキュリティ対策テーブル410の内容を示す図である。このセキュリティ対策テーブル410には、セキュリティ対策ID4100と、セキュリティホールに対するチェック条件4101と、チェック条件4101がYESの場合の処理内容を表すYES処理番号4102と、チェック条件4101がNOの場合の処理内容を表すNO処理番号4103が格納されている。

【0200】あるセキュリティホールに対するチェック条件が複数必要な場合には、このYES処理番号とNO処理番号に、セキュリティ対策IDが格納される場合もある。

【0201】図42はYES/NO処理テーブル420

の内容を示す図である。このYES/NO処理テーブル420は、処理番号4200、処理内容4201ととなる。

【0202】図43は管理テーブル430の内容を示す図である。この管理テーブル430には、ネットワーク管理システムの管理対象であるネットワークの管理者が登録されている。

【0203】図43において、4300は管理者のID、4301は管理名、4302は管理者の所属である。

【0204】図44は外部ユーザテーブル440の内容を示す図である。この外部ユーザテーブル440には、ネットワーク管理システムの管理対象外である外部ネットワークから、管理対象のネットワークに対して、アクセスを許諾されている外部ユーザが登録されている。

【0205】図44において、4400は外部ユーザのID、4401は外部ネットワーク名、4402はユーザ名、4403はユーザの所属である。

【0206】まず、ネットワーク管理システムは、上述の実施例に示したような処理、即ち、常時ネットワーク環境を監視し、セキュリティホールを検出し、ネットワーク構成画面上に検出したセキュリティホールの表示を行う処理と同時に、セキュリティホールを後述するセキュリティ対策処理に通知する機能を有する。従って、これから述べるセキュリティホールへの対策を行う処理は、このセキュリティ対策処理への通知が発生した時点から処理を開始する。

【0207】図45のフローチャートのステップ4500において、検出したセキュリティホールのセキュリティIDの通知を受け取る。次に、ステップ4501において、通知されたセキュリティIDを元に図40に示したセキュリティホールテーブル400を検索し、該当するセキュリティ対策IDを得る。

【0208】次に、ステップ4502において、ステップ4501で得たセキュリティ対策IDを元に、図41で示したセキュリティ対策テーブル410を検索し、セキュリティホールに対応したチェック条件を得る。

【0209】ステップ4503において、チェック条件がYESかどうかを判断する。その際、必要に応じて図21のプログラム起動ログテーブル210によりプロセスの稼働状況を確認したり、図43の管理者テーブル430によりセキュリティホールを発生させたのが管理者かどうか調査したり、図44の外部ユーザテーブル440によりアクセスを許諾された外部ユーザかどうかを調査したりする。

【0210】ステップ4503のチェック条件がYESだった場合は、ステップ4504において、YES処理に格納されている内容がセキュリティ対策IDの場合は、再度セキュリティ対策テーブル410の検索を行うために、ステップ4502の前に戻る。YES処理に格

納されている内容が処理番号になるまでこれを繰り返す。

【0211】YES処理に処理番号が格納されていると、次に、ステップ4505でその処理番号を元に図42YES/NOテーブル420を検索する。

【0212】また、ステップ4503のチェック条件がNOだった場合も同様に、ステップ4506において、NO処理に格納されている内容がセキュリティ対策IDの場合は、再度セキュリティ対策テーブル410の検索を行うために、ステップ4502の前に戻る。NO処理に格納されている内容が処理番号になるまでこれを繰り返す。

【0213】NO処理に処理番号が格納されていると、次に、ステップ4507でその処理番号を元に図42のYES/NO番号テーブル420を検索する。

【0214】ステップ4505、又はステップ4507でYES/NO処理テーブル420を検索して処理内容を得ると、次に、ステップ4508において、処理内容を実行してセキュリティ対策を行う。

【0215】

【発明の効果】以上説明したように、本発明においては、

(1) ソフトウェア的セキュリティホールを検出し、検出したソフトウェア的セキュリティホールをネットワーク構成図面上に表示するので、ネットワークにおけるセキュリティを確保することができる。

【0216】(2) また、ネットワーク及びネットワーク機器に対するアクセス状況を常時監視するので、外部からの侵入、内部での不正利用の発見を速やかに行うことができる。

【0217】(3) さらに、ネットワーク環境設定用ファイルの内容をアクセス許諾条件に基づき照合及び検査するので、適正なネットワーク利用環境の構築を容易に行うことができる。

【0218】(4) さらに、ネットワーク管理の対象となっているネットワーク機器をネットワーク構成図面上で識別可能な形式で表示させるので、安全なネットワーク環境を視覚的に簡単に把握することができる。

【図面の簡単な説明】

【図1】 本発明の一実施例にかかるネットワーク管理システムの構成を示すブロック図である。

【図2】 本実施例の論理的ネットワークの構成を説明するための模式的構成図である。

【図3】 本実施例の表示装置上へのネットワーク構成図面の表示例を示す図である。

【図4】 本実施例の被管理機器ID、接続情報、分類、遠隔操作、管理者の対応を表す被管理機器の情報を格納したデータベースの構成を示す図である。

【図5】 本実施例のネットワーク環境を維持するために必要なファイルが登録されているデータベースの構成

を示す図である。

【図6】 本実施例のパケットのヘッダ部の構造を説明するための模式図である。

【図7】 本実施例の電子計算機がどの被管理機器からアクセスされているか表示する処理手順を示すフローチャートである。

【図8】 本実施例の電子計算機へのアクセス状況に関する収集データの例を示す図である。

【図9】 本実施例の被管理機器を流れているパケットの通信プロトコル別の数量や数量比を表示する処理手順を示すフローチャートである。

【図10】 本実施例の被管理機器をながれているパケットのパケットサイズと通信プロトコルを収集したデータの例を示す図である。

【図11】 本実施例の通信プロトコル別のパケットサイズ合計を示す棒グラフである。

【図12】 本実施例の通信プロトコル別のパケットサイズ合計の数量比を円グラフを用いて表示した例である。

【図13】 本実施例の指定した端末で、どのユーザ名でこの電子計算機にログインしているかを調査して表示する処理手順を示すフローチャートである。

【図14】 本実施例のログイン記録テーブルの例を示す図である。

【図15】 本実施例の指定した端末で、どのユーザ名でこの電子計算機にログインしているかを示す検出結果の表示例である。

【図16】 本実施例のネットワーク環境維持ファイルへのアクセス履歴を保存するために、予め、実行する処理手順を示すフローチャートである。

【図17】 本実施例のネットワーク環境維持ファイルへのアクセス履歴を表示する処理手順を示すフローチャートである。

【図18】 本実施例のネットワーク環境維持ファイルへのアクセス履歴の例を示す図である。

【図19】 本実施例のネットワーク環境維持ファイルへのアクセス履歴の表示例を示す図である。

【図20】 本実施例の特権モードで稼働中のプログラムを捜し出して表示する処理手順を示すフローチャートである。

【図21】 本実施例のプログラム起動ログテーブルの例を示す図である。

【図22】 本実施例の特権モードで稼働中のプログラムを検出した結果の表示例を示す図である。

【図23】 本実施例のある期間に誰がどの端末で特権ユーザとなり、どのようなプログラムを動かしたかを調査し表示する処理手順を示すフローチャートである。

【図24】 本実施例のある期間に特権ユーザでログインした時間帯や端末名等をログイン記録テーブルから検出した結果の例である。

【図25】 本実施例のある期間に誰がどの端末で特権ユーザとなり、どのようなプログラムを動かしたかを検出した結果の表示例である。

【図26】 本実施例のネットワーク環境維持ファイルのアクセス権を検査する処理手順を示すフローチャートである。

【図27】 本実施例のネットワーク環境維持ファイルのアクセス権の本来あるべき設定を表すデータベースの例を示す図である。

【図28】 本実施例のアクセス権の設定を説明する概念図である。

【図29】 本実施例のネットワーク環境維持ファイルのアクセス権を収集した例を示す図である。

【図30】 本実施例のネットワーク環境維持ファイルのアクセス権を検査した結果の例を示す図である。

【図31】 本実施例の一般ユーザが特権モードで起動できるプログラムを探し出して表示する処理手順を示すフローチャートである。

【図32】 本実施例のプログラム状態テーブルの例を示す図である。

【図33】 本実施例の事前登録テーブルの例を示す図である。

【図34】 本実施例の一般ユーザが特権モードで起動できるプログラムを検出した結果の表示例である。

【図35】 本実施例の監視プログラムが稼働しているかを調査して表示する処理手順を示すフローチャートである。

【図36】 本実施例の監視プログラム登録テーブルの例を示す図である。

【図37】 本実施例の調査対象となるコンピュータを

指定する例を示す図である。

【図38】 本実施例の調査対象の範囲を指定する例を示す図である。

【図39】 本実施例の指定した監視プログラムが全て稼働中であるかどうかの表示例を示す図である。

【図40】 本発明の一実施例にかかるネットワーク管理システムのセキュリティホールテーブルの内容を示す図である。

【図41】 本発明の一実施例にかかるネットワーク管理システムのセキュリティ対策テーブルのないようを示す図である。

【図42】 本発明の一実施例にかかるネットワーク管理システムのYES/NO処理テーブルの内容を示す図である。

【図43】 本発明の一実施例にかかるネットワーク管理システムの管理者テーブルの内容を示す図である。

【図44】 本発明の一実施例にかかるネットワーク管理システムの外部ユーザテーブルの内容を示す図である。

【図45】 本発明の一実施例にかかるネットワーク管理システムの検出したセキュリティホールへの対策を行う処理手順を示すフローチャートである。

【符号の説明】

100…ネットワーク、101…通信制御装置、102…中央処理装置、103…入力装置、104…出力装置、105…補助記憶装置、200…通信網、201…電子計算機、202…ネットワーク機器、203…端末、300…通信網、301…ネットワーク機器、302…電子計算機、303…端末。

【図4】

図4

被管理機器ID	接続情報	分類	遠隔操作	管理者
000001	000010	電子計算機	○	mriko
023206	023207, 023208	ケーブル類	×	tage
398730	398729, 398731	ネットワーク機器	○	ack
⋮	⋮	⋮	⋮	⋮

40

【図5】

図5

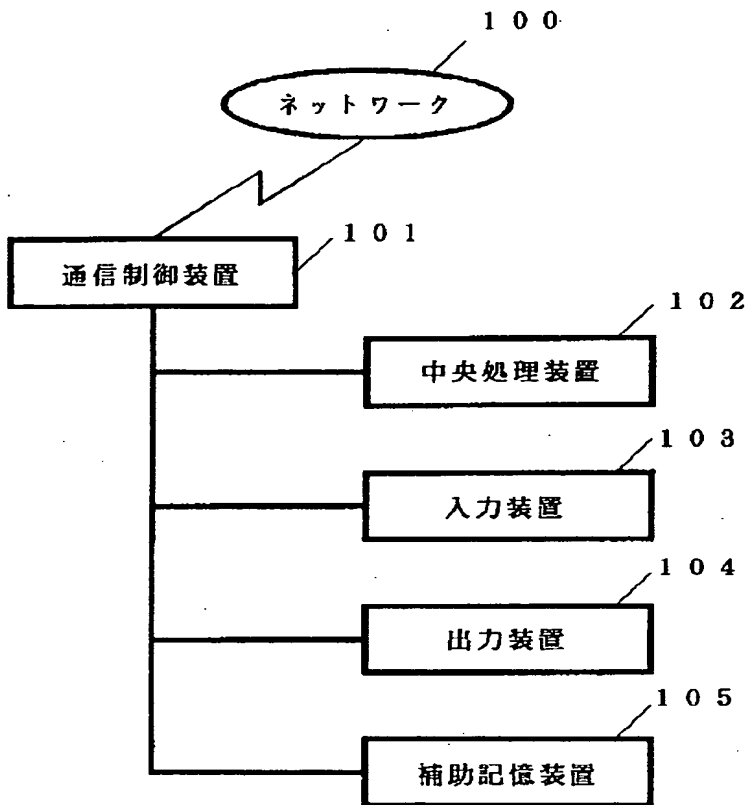
ネットワーク環境 維持ファイル
/etc/passwd
/etc/group
/etc/rc
⋮

50



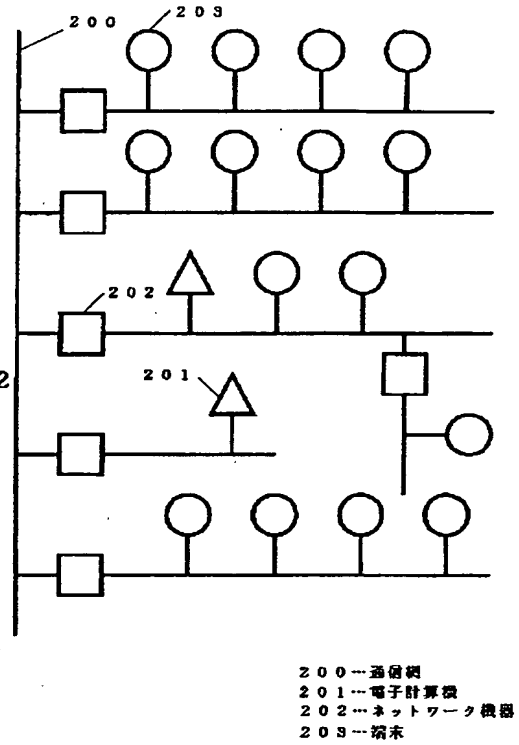
【図1】

図 1



【図2】

図 2



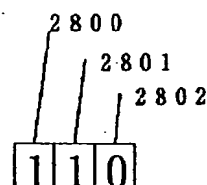
【図8】

図 8

受信先 被管理機器ID	送信元 被管理機器ID	通信プロトコル
000001	002387	プロトコル1
874983	000001	プロトコル2
398730	000001	プロトコル3
⋮	⋮	⋮

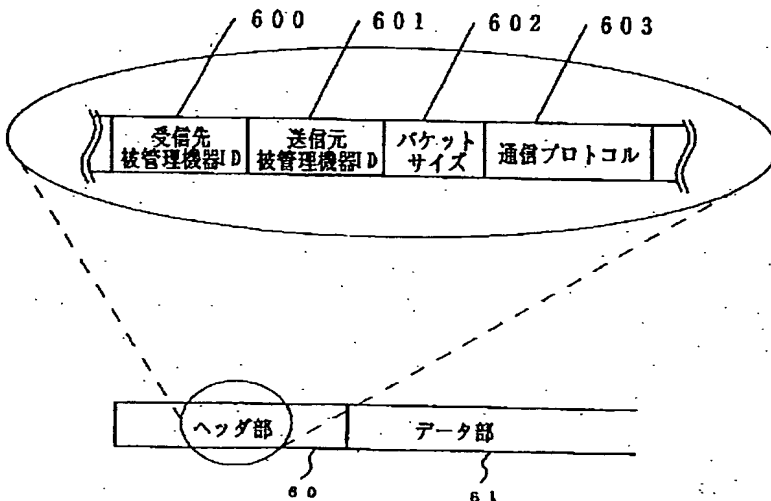
【図28】

図 28



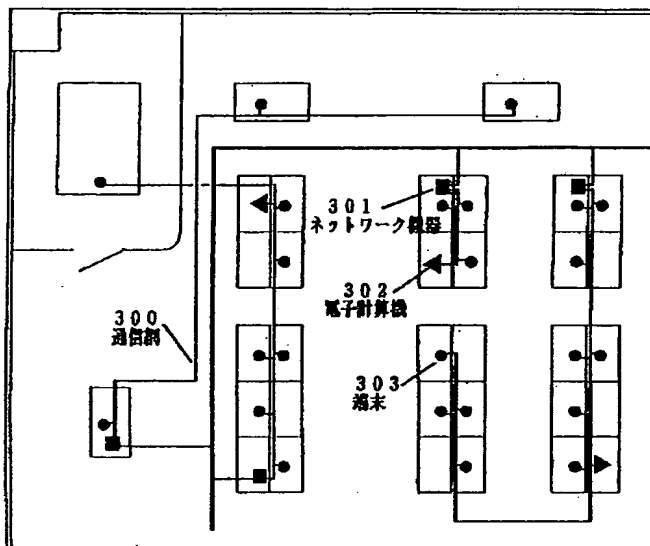
【図6】

図 6



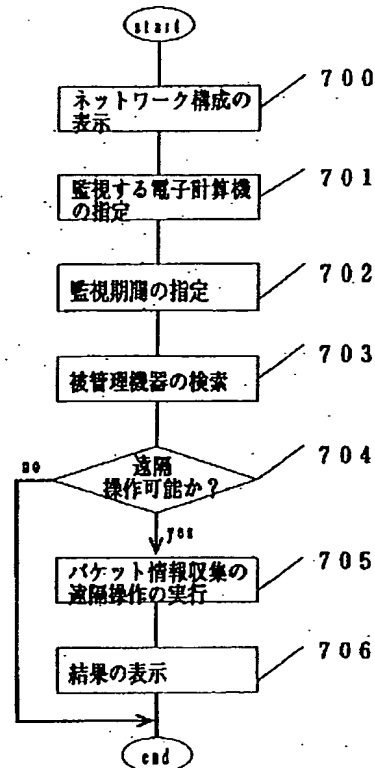
【図3】

図3



【図7】

図7



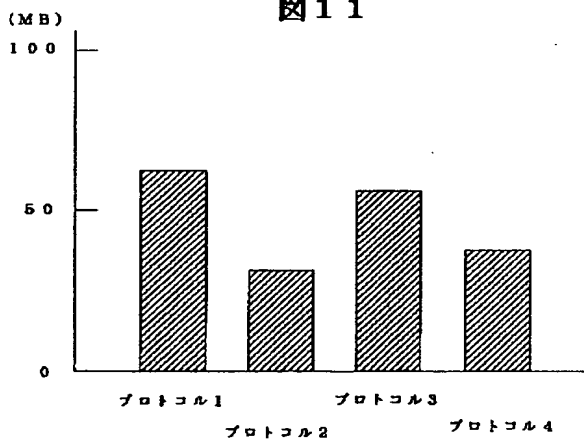
【図10】

図10

1000	1001
パケットサイズ	通信プロトコル
1500	プロトコル1
23	プロトコル2
125	プロトコル3
⋮	⋮

【図11】

図11



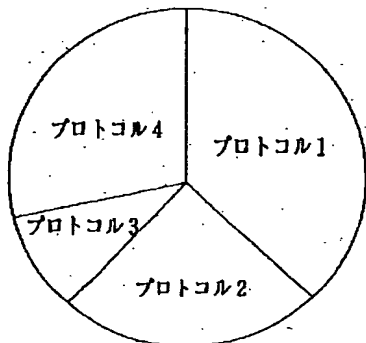
【図43】

図43

管理者テーブル		
4300	4301	4302
ID	管理者 名	所属
101	佐藤 花子	設計
102	田中 次郎	企画
⋮	⋮	⋮

【図12】

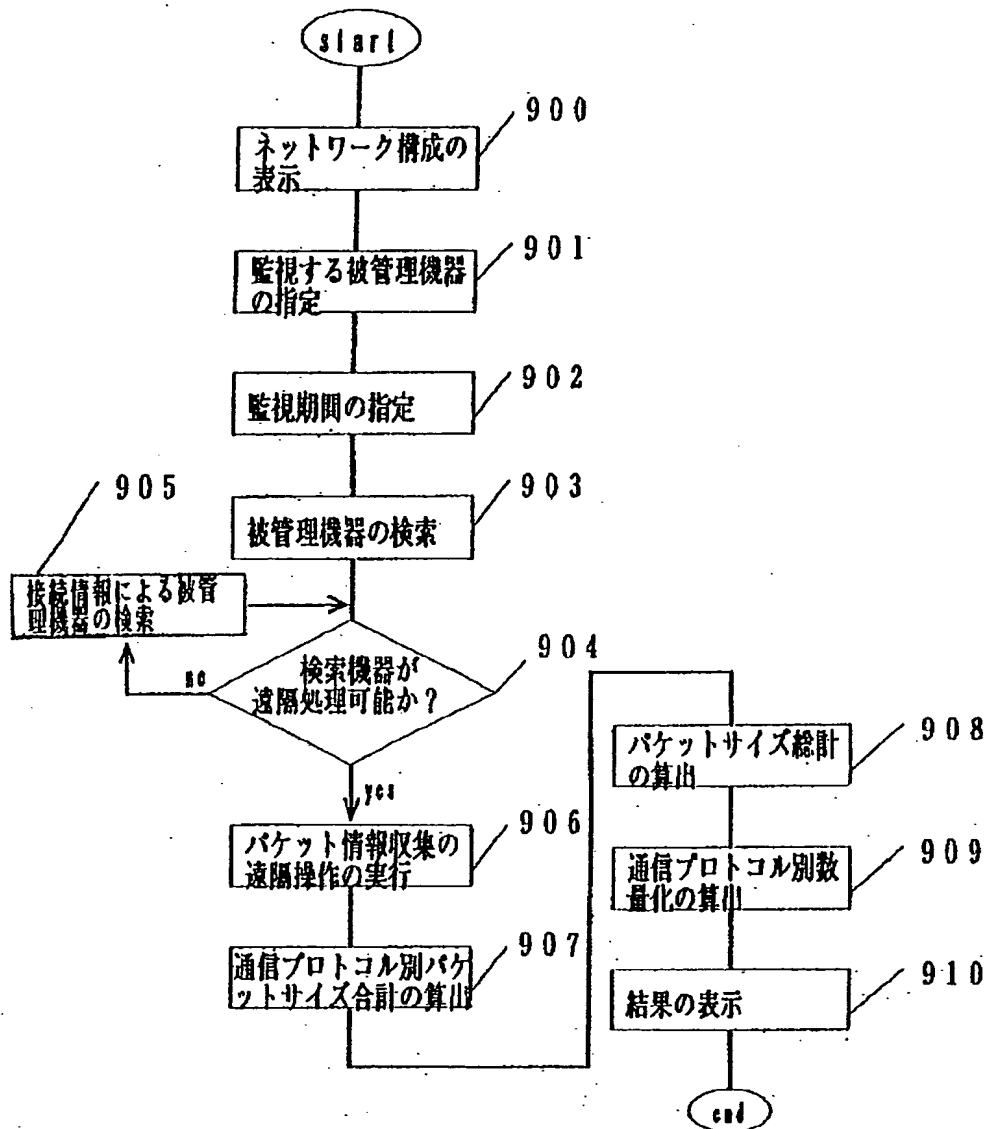
図12



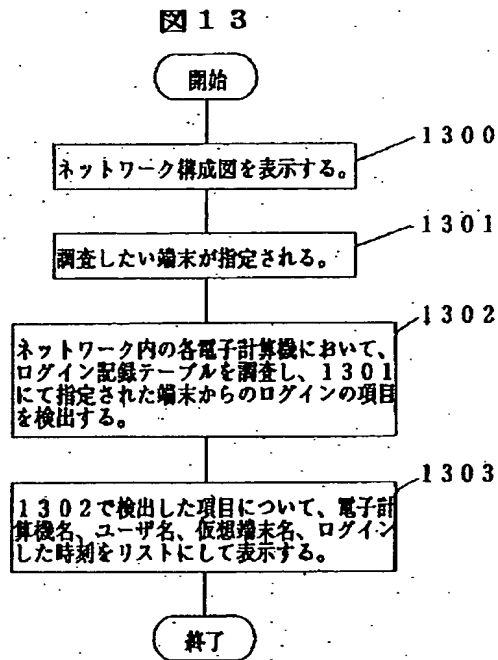
430

【図 9】

図 9



【図13】

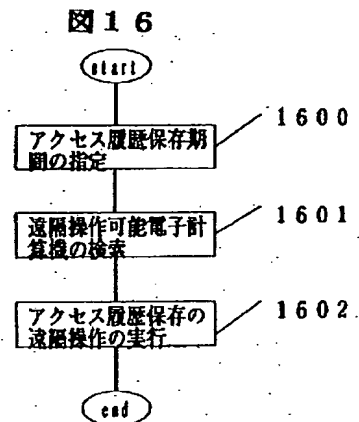


【図15】

図15

1500 電子計算機名	1501 ユーザ名	1502 仮想端末名	1502 ログインした時刻
電子計算機1	USER2	tty3	92.11.1. 10:10:00
電子計算機2	root	tty1	92.11.1. 10:20:30
⋮	⋮	⋮	⋮

【図16】

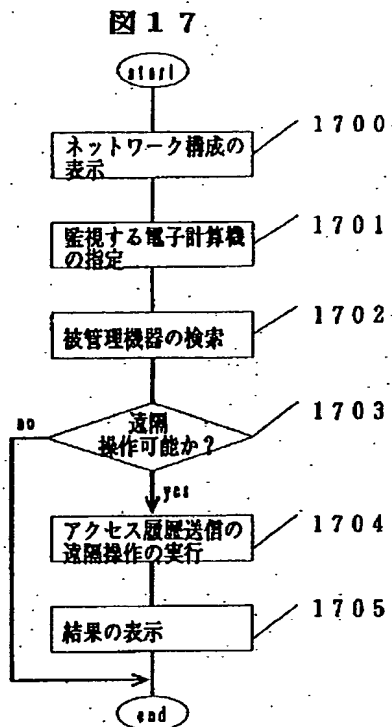


【図14】

図14

1400 ログインしたユーザ名	1401 使用した仮想端末名	1402 ログインした端末名	1403 ログインした時刻	1404 ログアウトした時刻	1405 ログインする前のユーザ名
USER2	tty3	端末1	92.11.1. 10:10:00		
USER3	tty2	端末2	92.11.1. 10:15:05	92.11.1. 12:10:00	USER6
root	tty1	端末1	92.11.1. 10:20:30	92.11.1. 10:40:30	USER2
user1	tty7	端末3	92.11.1. 10:23:10	92.11.1. 12:40:43	
root	tty4	端末4	92.11.1. 10:29:00	92.11.1. 11:00:00	
⋮	⋮	⋮	⋮	⋮	⋮

【図17】



【図18】

図18

1800 アクセスユーザ	1801 アクセス方法	1802 アクセス日時
nak	read	92/05/30
mariko	write	92/06/01
yamiko	write	92/08/16
⋮	⋮	⋮

180

【図32】

図32

3200 プログラム名	3201 プログラムの所有者	3202 起動可能なユーザ	3203 稼働時のモード
prog1	root	全ユーザ	特権
prog2	user1	user1	一般
prog3	root	root	特権
⋮	⋮	⋮	⋮

320

【図19】

図19

ファイル名	アクセスユーザ	アクセス方法	アクセス日時
/etc/passwd	nak	read	92/05/30
/etc/group	mariko	write	92/06/01
/etc/hosts	yamiko	write	92/08/16
⋮	⋮	⋮	⋮

【図34】

図34

3400 プログラム名	3401 プログラムの所有者	3402 起動可能なユーザ
prog1	root	全ユーザ
⋮	⋮	⋮

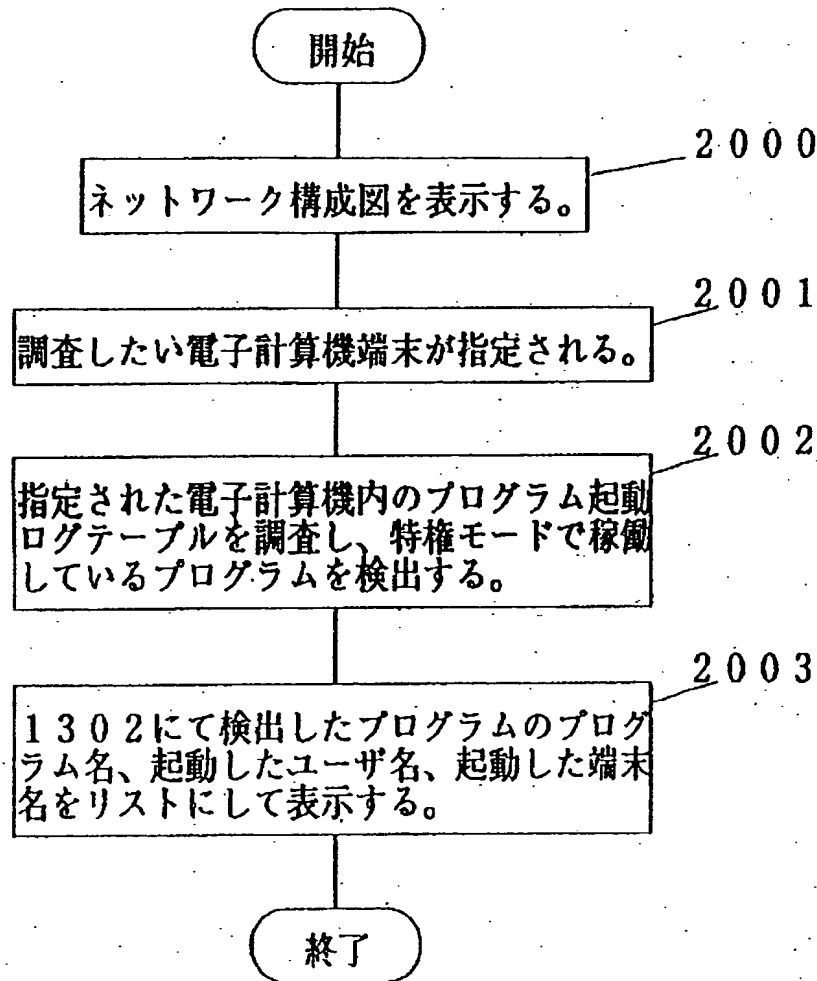
【図22】

図22

2200 プログラム名	2201 ユーザ名	2202 起動した仮想端末名	2203 起動した端末名	2204 起動時刻
user2	prog1	tty3	端末1	92.11.1. 10:15:30
user1	prog1	tty7	端末3	92.11.1. 10:24:00
root	prog3	tty4	端末4	92.11.1. 10:29:15
⋮	⋮	⋮	⋮	⋮

【図20】

図 2 0



【図24】

図 2 4

2400 仮想端末名	2401 端末名	2402 ログインしていた時間帯	2403 特権ユーザにログインしたユーザ名
tty1	端末1	92.11.1. 10:20:30 ~ 10:40:30	user2
tty4	端末4	92.11.1. 10:29:00 ~ 10:50:00	
⋮	⋮	⋮	⋮

【図21】

【図36】

図21

図36

2100 起動した ユーザ名	2101 起動したプ ログラム名	2102 起動した仮 想端末名	2103 起動した端 末名	2104 起動時刻	2105 終了時刻	2106 起動時の モード
user2	prog10	tty3	端末1	92.11.1. 10:11:00	92.11.1. 10:11:30	一般
user2	prog1	tty3	端末1	92.11.1. 10:14:30		特権
user3	prog15	tty2	端末2	92.11.1. 10:16:30		一般
user1	prog1	tty7	端末3	92.11.1. 10:24:00		特権
root	prog1	tty1	端末1	92.11.1. 10:25:00	92.11.1. 10:26:00	特権
root	prog3	tty4	端末4	92.11.1. 10:29:15		特権
⋮	⋮	⋮	⋮	⋮	⋮	⋮

3600 電子計算機名	3601 監視プログラム名	3602 重要度
電子計算機1	login-check	大
電子計算機1	police	小
電子計算機1	program-check	大
電子計算機2	login-check	大
⋮	⋮	⋮

210

360

【図25】

図25

2500 仮想端末名	2501 ログインし た端末名	2502 起動したプ ログラム名	2503 起動時刻	2504 終了時刻	2505 ログインをし たユーザ名
tty1	端末1	prog1	92.11.1. 10:25:00	92.11.1. 10:26:00	user2
tty4	端末4	prog3	92.11.1. 10:29:15		
⋮	⋮	⋮	⋮	⋮	⋮

【図27】

【図42】

図27

図42

2700 ファイル名	2701 ユーザ アクセス	2702 グループ アクセス	2703 その他 アクセス	2704 所有者	2705 所有者の グループ
/etc/passwd	100	100	100	root	system
/etc/group	100	100	100	root	system
/etc/hosts	100	100	100	root	system
⋮	⋮	⋮	⋮	⋮	⋮

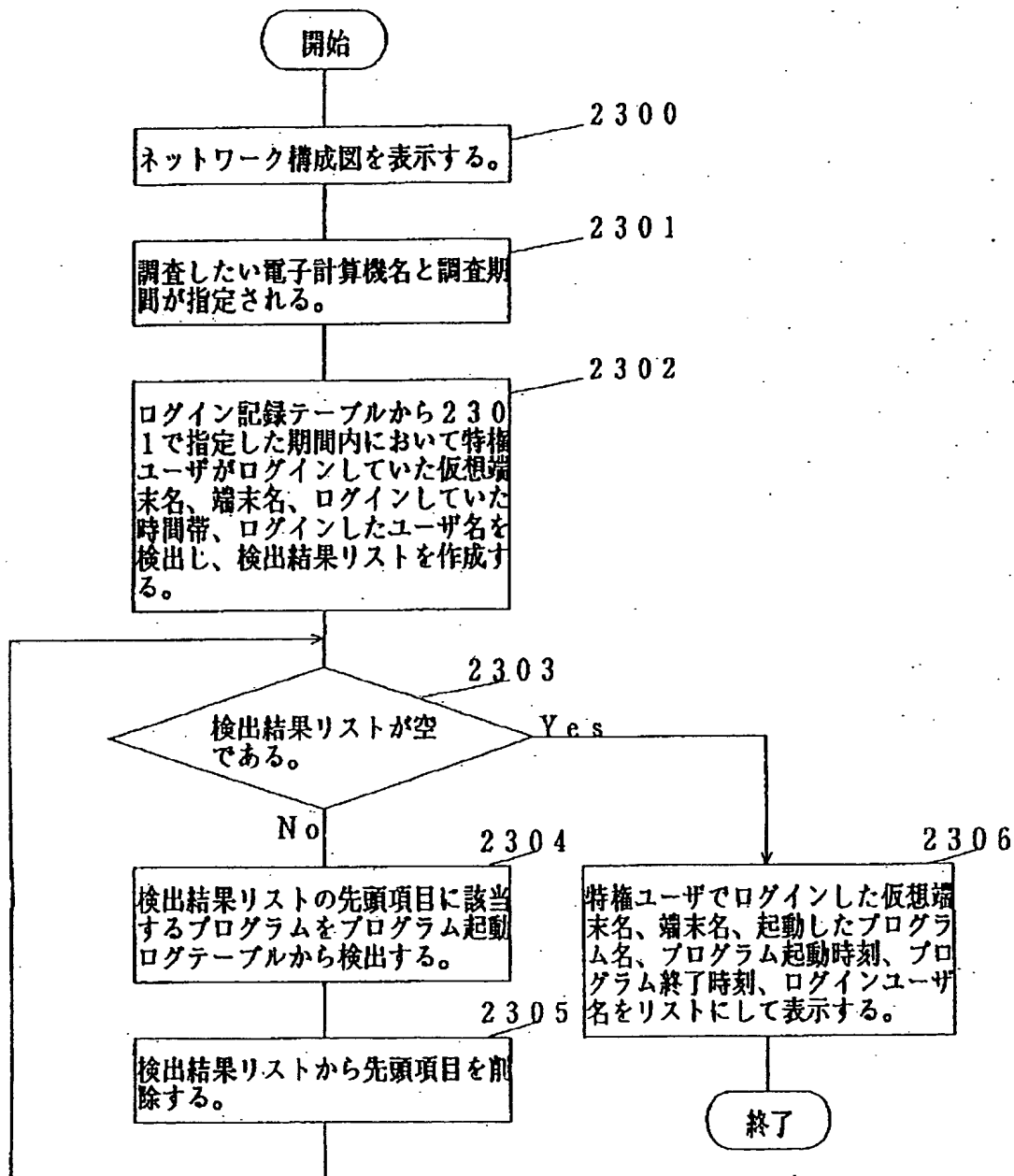
4200 処理番号	4201 処理内容
100	管理者にセキュリティホール の内容をメール送信
200	該当プロセスを消去
300	該当アカウントのユーザに 警告メールを送信
⋮	⋮

270

420

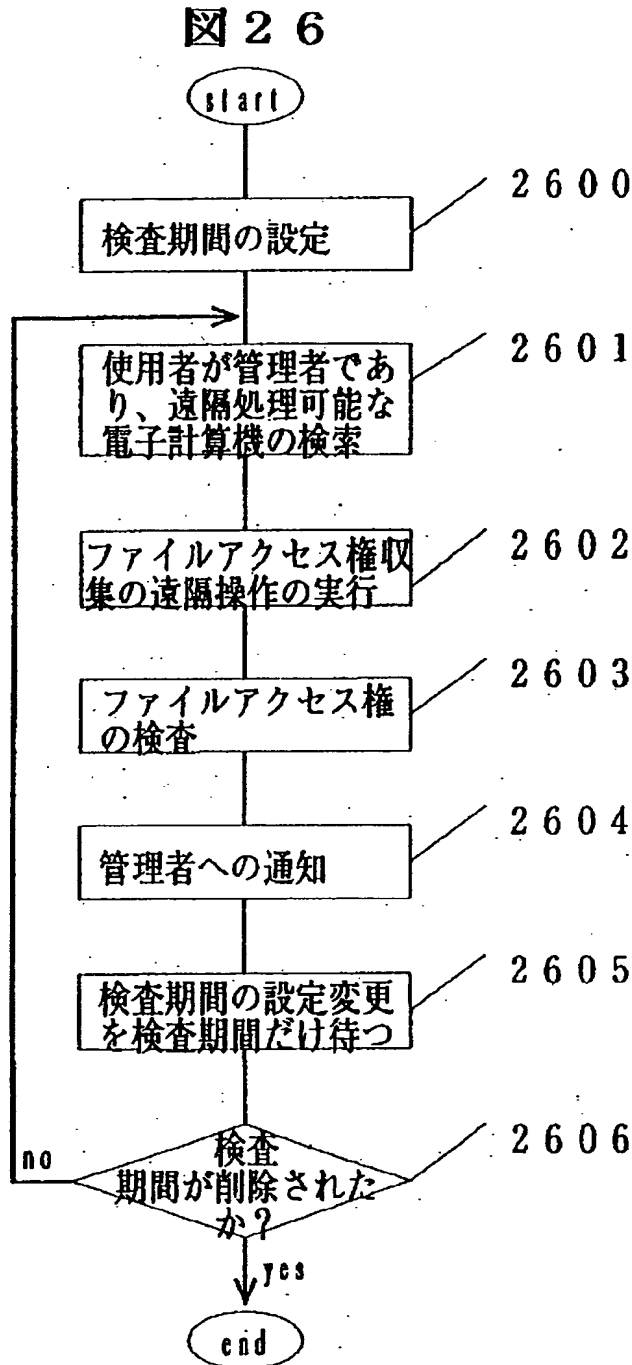
【図23】

図 2 3





【図 2 6】



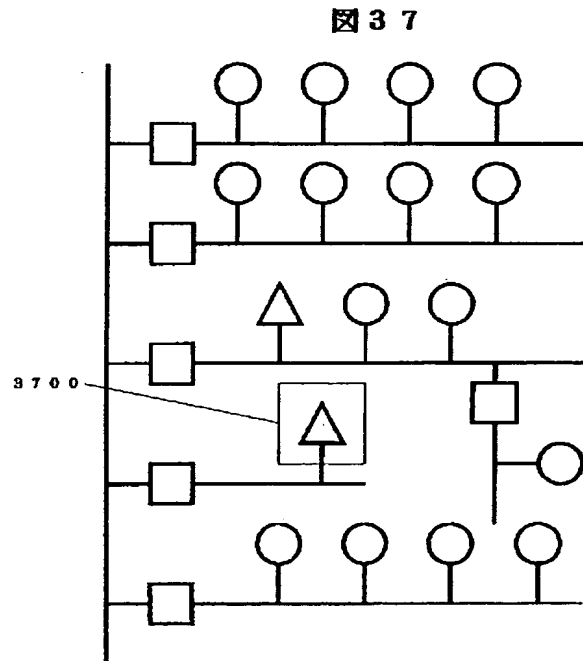
【図 3 3】

**図 3 3**

プログラム名	プログラムの所有者	起動可能なユーザ	稼働時のモード
prog1	root	root	特権
prog1	root	root	特権
⋮	⋮	⋮	⋮

330

【図 3 7】



【図29】

図29

ファイル名	ユーザ アクセス	グループ アクセス	その他 アクセス	所有者	所有者の グループ
/etc/passwd	110	110	000	mariko	network
/etc/group	110	100	000	nak	DB
/etc/hosts	110	000	100	root	system
⋮	⋮	⋮	⋮	⋮	⋮

【図30】

図30

ファイル名	ユーザ アクセス	グループ アクセス	その他 アクセス	所有者	所有者の グループ
/etc/passwd	110	110	000	mariko	network
	110	110	100	root	system
⋮	⋮	⋮	⋮	⋮	⋮

300

【図41】

図41

セキュリティ対策テーブル

セキュリティ対策ID	チェック内容	YES 処理	NO 処理
A	プロセスが稼働中である	200	300
B	ユーザは管理者である	400	100
C	外部ユーザが認可されている	E	D
⋮	⋮	⋮	⋮

410

【図44】

図44

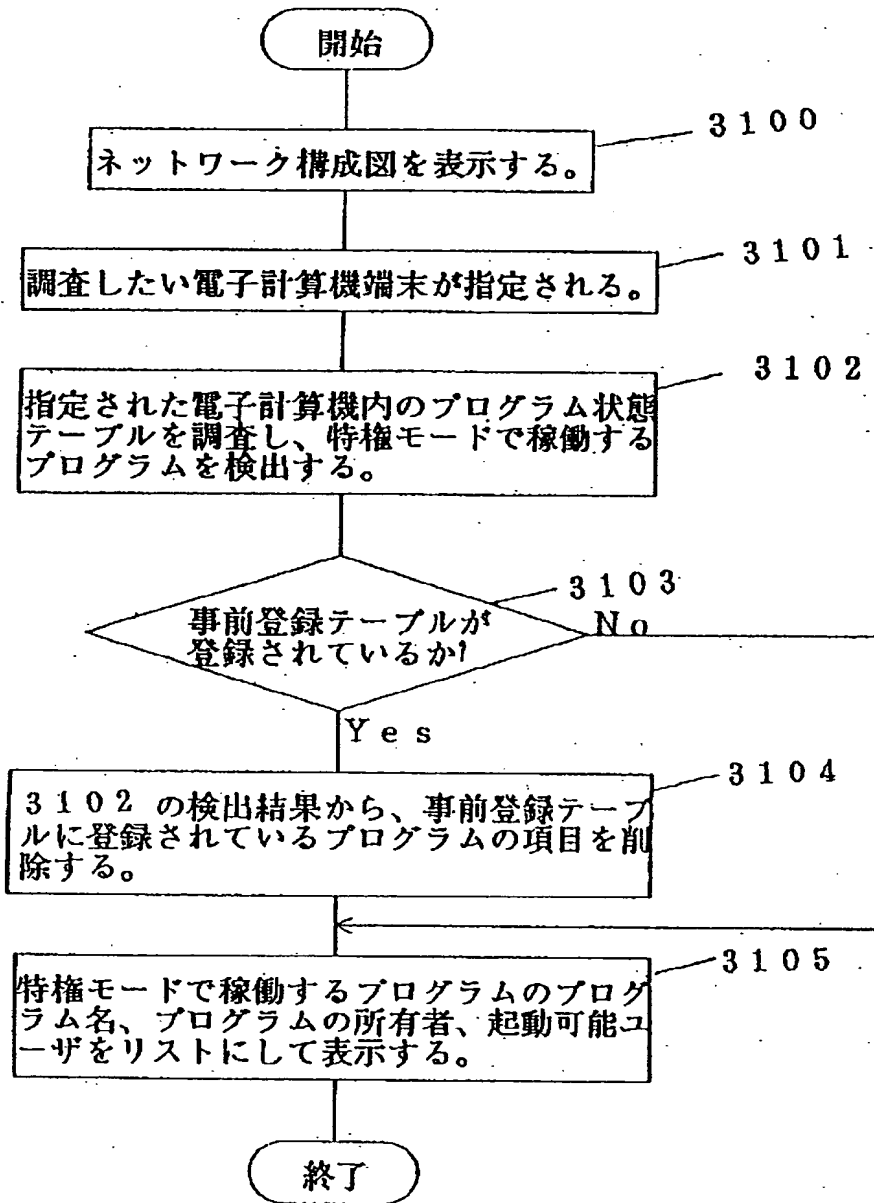
外部ユーザテーブル

ID	外部ネットワーク	ユーザ名	所属
1000	A大学	鈴木教授	理学部
1001	B電気会社	斉藤部長	システム部
⋮	⋮	⋮	⋮

440

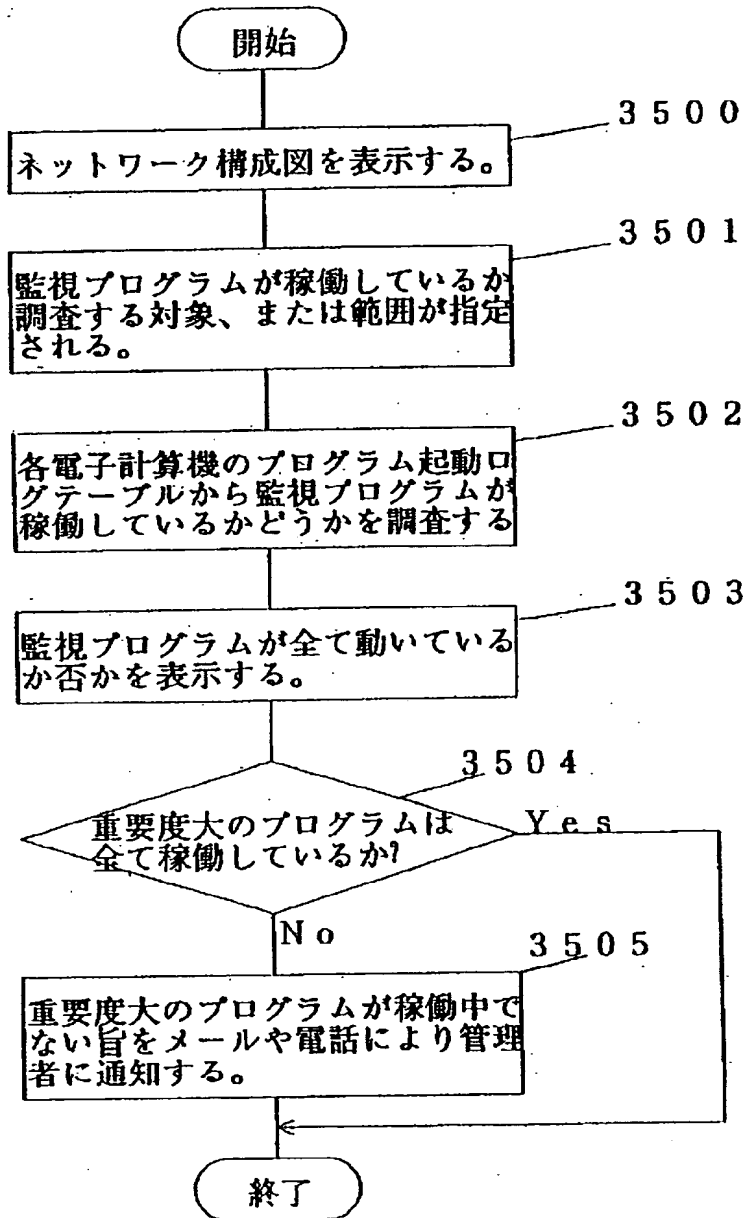
【図31】

## 図 3 1



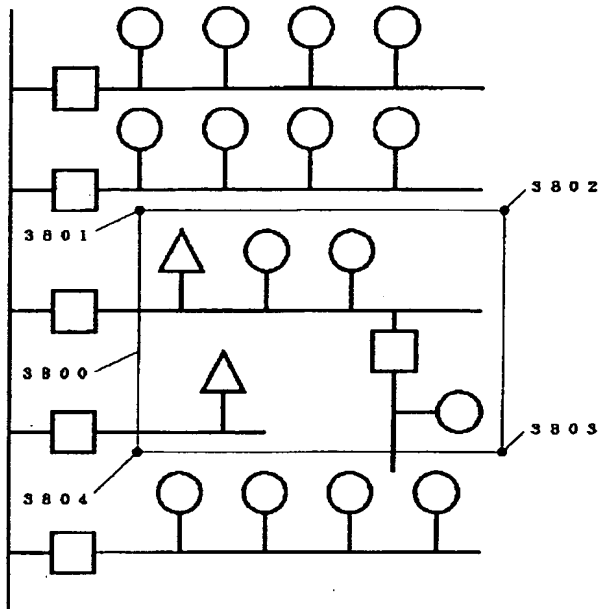
【図35】

図 3 5



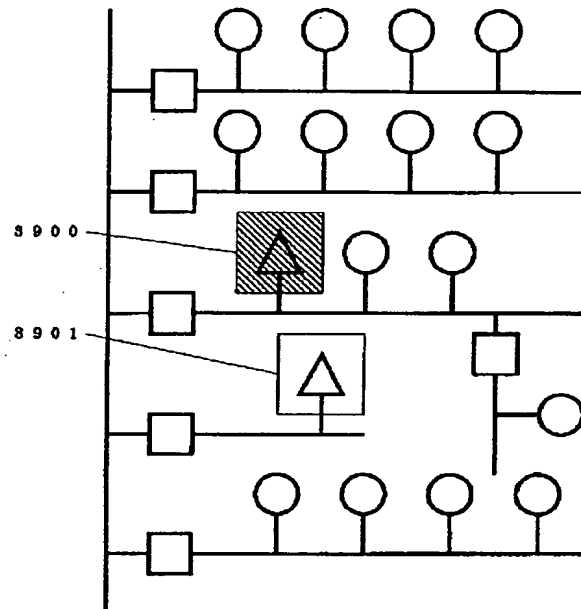
【図38】

図 38



【図39】

図 39



【図40】

図 40

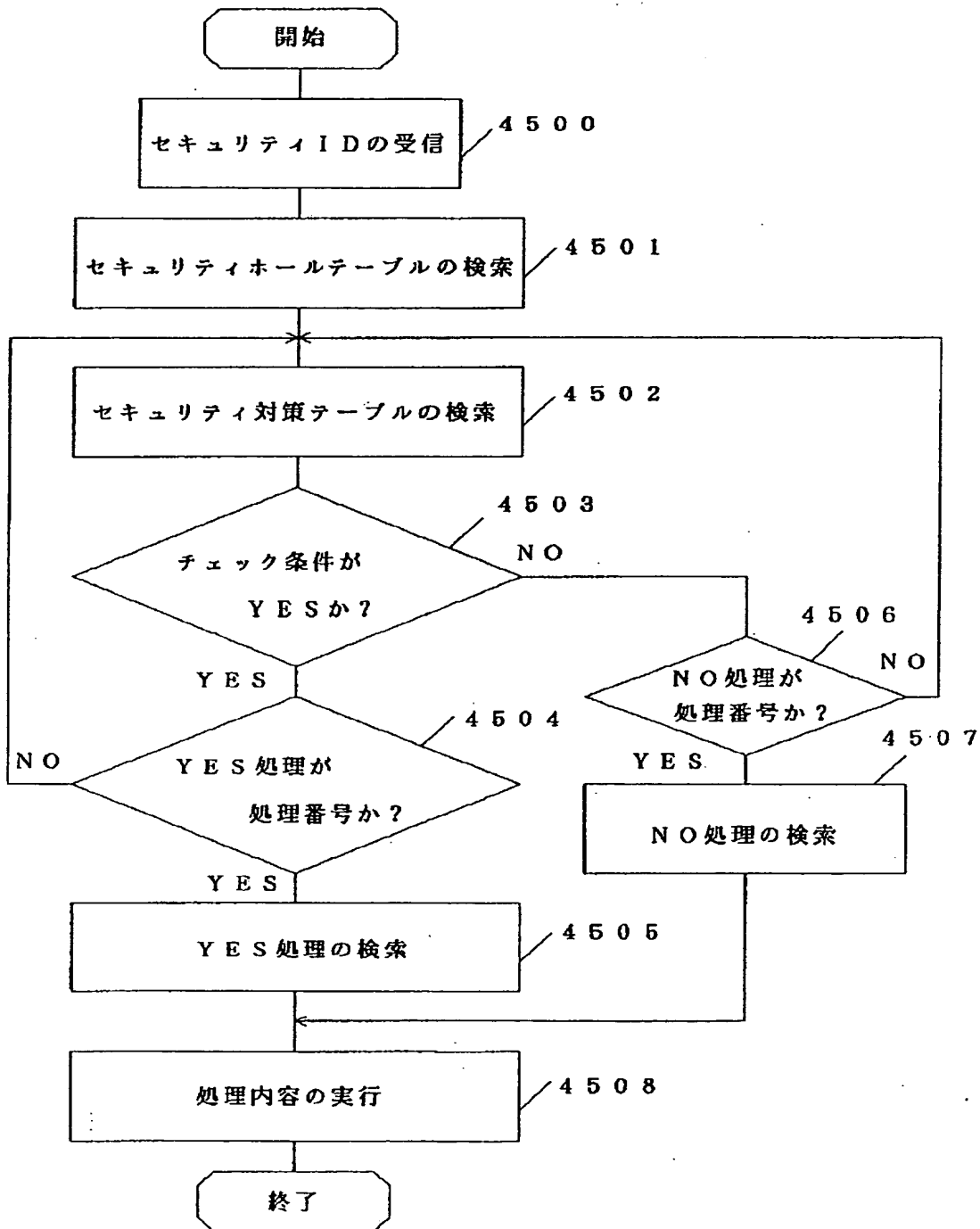
セキュリティホールテーブル

セキュリティID	セキュリティホールの内容	セキュリティ対策ID
1	不正アカウントのユーザ	A
2	不正な特権モードプロセスあり	B
3	外部ネットワークからの ログイン試行あり	C
...	...	...

400

【図45】

## 図 4 5



フロントページの続き

(51) Int. Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
12/26				
H04M 3/42	E	8732-5K	H04L 11/08	

(72) 発明者 堤 俊之  
神奈川県横浜市中区尾上町6丁目81番地  
日立ソフトウェアエンジニアリング株式会  
社内